ST. PETERSBURG INSTITUTE
FOR INFORMATICS AND AUTOMATION
(SPIIRAS)

EUROPEAN OFFICE OF AEROSPACE
RESEARCH AND DEVELOPMENT
(EOARD)

Agent-Based Model of Information Security System: Architecture and Formal Framework for Coordinated Intelligent Agents Behavior Specification

Final Report #2

!"#$%&'()(*+,+(!

Project Manager
Chief Scientist of SPIIRAS
Ph.D. Professor
V.I. Gorodetski

St. Petersburg
February 2001

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
21-03-2001

2. REPORT TYPE
Final Report

3. DATES COVERED *(From – To)*
12/1/1999 - 01-Mar-01

4. TITLE AND SUBTITLE

Agent-Based Model of Information Security System: Architecture and Formal Framework for Coordinated Intelligent Agents Behavior Specification

5a. CONTRACT NUMBER
ISTC Registration No: 1686

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Dr. Vladimir Gorodetski

5d. PROJECT NUMBER

5d. TASK NUMBER

5e. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
St. Petersburg Institute For Informatics & Automation of the Russian Academy of Sciences
39, 14th Liniya
St. Petersburg 199178
Russia

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

EOARD
PSC 802 BOX 14
FPO 09499-0014

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
ISTC 99-7001

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The contractor will research and further develop the technology supporting an agent-based architecture for an information security system and a formal framework to specify a model of distributed knowledge. This research will include a comparative analysis of existing steganography & steganoanalysis techniques and the development and mathematical justification of an alternative approach to be incorporated in the proposed architecture.

15. SUBJECT TERMS
EOARD, Mathematical & Computer Sciences, Cybernetics

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18, NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**Chris Reuter**
UNCLAS	UNCLAS	UNCLAS	UL	three parts 59 pages	**19b. TELEPHONE NUMBER** *(Include area code)* **+44-20-7514-4474.**

Contents

Preface

O2A5(I#C7@%(A5('2%(YA</C(J%3#"'()-(#<('2%(!"#$%&'()*+,+(!('2/'(A5(>%A<;(&/""A%8(#7'(/&&#"8A<;
'#('2%(/;"%%@%<'(>%'F%%<(R7"#3%/<(H..A&%(#.(:%"#53/&%(J%5%/"&2(/<8(M%I%C#3@%<'(ZRH:JM[E
O2%(?<'%"</'A#</C(6&A%<&%(/<8(O%&2<#C#;9(1%<'%"(Z?6O1[(/<8(6'4(!%'%"5>7";(?<5'A'7'%(.#"
?<.#"@/'A&5(/<8(:7'#@/'A#<(#.('2%(J755A/<(:&/8%@9(#.(6&A%<&%5(Z6!??J:6[4(O2%(!"#$%&'('A'C%(A5

\Agent-Based Model of Information Security System: Architecture and Formal Framework for Coordinated Intelligent Agents Behavior Specification".

O2A5("%3#"'(57@@/"A]%5('2%("%57C'5(#.('2%(.A.'2(32/5%(#.("%5%/"&2(5&2%87C%8(>9('2%(^#"P(!C/<
/5(F%CC(/5(57@@/"A]%('2%("%5%/"&2("%57C'5(#<('2%(!"#$%&'(#<(/(F2#C%4

:&&#"8A<;('#('2%(^#"P(!"#;"/@E(/'('2A5(32/5%(#.("%5%/"&2('2%(.#CC#FA<;('/5P(A5(5&2%87C%8B

:4,4M%I%C#3@%<'(/<8(%S3C#"/'A#<(#.('2%(5#.'F/"%(A@3C%@%<'/'A#<(#.(/(&/5%(5'789(#.(/;%<'=
>/5%8(?<.#"@/'A#<(6%&7"A'9(695'%@(Z?66[4

?<('2A5(J%3#"'(12/3'%"(*(3"%5%<'5('2%(@/A<("%5%/"&2("%57C'5(#<('2%('/5P(:4,E(A4%4(A'(8%5&"A>%5
&#<&%3'7/C(@#8%CE(/"&2A'%&'7"%(/<8(5#.'F/"%(A@3C%@%<'/'A#<(#.('2%(&/5%(5'789(#.('2%(@7C'A=/;%<'
<%'F#"P(5%&7"A'9(595'%@4(?<(/88A'A#<E(A'(;AI%5('2%(;%<%"/C(&#<&C75A#<(&#<&%"<A<;('2%(%<'A"%("%5%/"&2
&/""A%8(#7'(/&&#"8A<;('#('2%(!/"'(*(/<8(!/"'(-(#.('2%(!"#$%&'4

12/3'%"(-(57@@/"A]%5('2%(@/A<("%5%/"&2("%57C'5('2/'(&#<&%"<('#('2%(MA;A'/C(?@/;%
6'%;/<#;"/329 4(?<(./&'E('2A5(12/3'%"(#I%"C/35(FA'2('2%(12/3'%"(-(#.('2%(3"%IA#75(J%3#"'E(A4%4
12/3'%"(-(#.('2%(YA</C(J%3#"'()*4(_%I%"'2%C%55E(F%(&#<5A8%"('2/'(A'(A5(<%&%55/"9('#(57@@/"A]%('2%5%
"%57C'5(/5('2%(.A</C(&#<&C75A#<(#<('2%(5'%;/<#;"/329=#"A%<'%8(!"#$%&'("%5%/"&24

:CC('2%#"%'A&/C("%57C'5(/<8(&#<&C75A#<5(#.('2%("%5%/"&2(/"%(%S3C#"%8(/<8(I/CA8/'%8(IA/
5A@7C/'A#<(#<('2%(>/5A5(#.('2%(5#.'F/"%(8%I%C#3%8(>9(/7'2#"54(O2%(8%I%C#3%8(5#.'F/"%(FACC(>%
8%@#<5'"/'%8(A<(:YJ`a?O(/<8(5#.'F/"%(&#8%(FACC(>%(57>@A''%8('#('2%(!/"'<%"(#<(8%@/<84

:CC('/5P5(3"%5733#5%8(>9('2%(^#"P(!"#;"/@(/"%(5#CI%8(&#@3C%'%C94

!"#$%&'(@/</;%"
12A%.(6&A%<'A5'(#.('2%(6'4(!%'%"5>7";(?<5'A'7'%
.#"(?<.#"@/'A&5(/<8(:7'#@/'A#<(#.('2%
J755A/<(:&/8%@9(#.(6&A%<&%5

!24M4(!"#.4(WC/8A@A"(X#"#8%'5PA

Chapter 1. Case Study of Agent-based Information Security System: Conceptual Model, Architecture, Software Implementation and Simulation

Abstract.(O2%(12/3'%"(&#<5A8%"5('2%(8%I%C#3%8(1/5%(6'789(#.('2%(&#@37'%"(<%'F#"P(5%&7"A'9 595'%@('2/'(A5(A@3C%@%<'%8(/5(@7C'A=/;%<'(595'%@4(O2%(1/5%(6'789(A5(&#@3#5%8(#.(3/'"A&7C/" /7'#<#@#75(P<#FC%8;%=>/5%8(/;%<'5E(8A5'"A>7'%8(#I%"('2%(2#5'5(#.('2%(&#@37'%"(<%'F#"P('#(>% 3"#'%&'%8(/<8(&##3%"/'A<;('#(@/P%(A<'%;"/'%8(&#<5A5'%<'(8%&A5A#<54(O2%(12/3'%"(8%5&"A>%5('2% /"&2A'%&'7"%(#.('2%(5%&7"A'9(595'%@(1/5%(6'789(/<8(/"&2A'%&'7"%5(#.(A'5(&#@3#<%<'5('2/'(/"% 3/"'A&7C/"(5#.'F/"%(/;%<'5E(&#@@7<A&/'A#<(&#@3#<%<'5(/<8(5#.'F/"%(5A@7C/'A<;('2%(A<37' '"/..A&4(O2%(1/5%(6'789(/"&2A'%&'7"%(&#""%53#<85('#('2%(@7C'A=/;%<'(595'%@(3"#'%&'A<;(/(`#&/C :"%/(_%'F#"P4(R/&2(2#5'=>/5%8(&#@3#<%<'(#.('2%(<%'F#"P(5%&7"A'9(595'%@(&#@3"A5%5(5%I%< 53%&A/CA]%8(5#.'F/"%(/;%<'5(5A'7/'%8(#<('2%(2#5'4

O2A5(1/5%(6'789(A5(A@3C%@%<'%8(/5(8A5'"A>7'%8(@7C'A=/;%<'(595'%@(F2A&2(&#@3#<%<'5(A<'%"/&' IA/(@%55/;%(%S&2/<;%4(6A@7C/'A#<(5&%</"A#E(A<37'('"/..A&(@#8%C(/<8(3%&7CA/"A'A%5(#.('2% 8A5'"A>7'%8(5%&7"A'9(595'%@(#3%"/'A#<(/"%(8%5&"A>%84(O2%(@/$#"(/''%<'A#<(A5(3/A8('#('2%(A<'"75A#< 8%'%&'A#<('/5P(/<8(/;%<'5(A<'%"/&'A#<5(87"A<;(8%'%&'A#<(#.(/<(/''/&P(/;/A<5'('2%(&#@37'%" <%'F#"P4(1/5%(6'789(A@3C%@%<'/'A#<(F/5(&/""A%8(#7'(#<('2%(>/5A5(#.('2%(D7C'A=/;%<'(695'%@ M%I%C#3@%<'(bA'(8%I%C#3%8(>9(/7'2#"5(#.('2%("%5%/"&24(?@3C%@%<'/'A#<('%&2<#C#;9(A5(#7'CA<%8 /5(F%CC4(O2%(5#.'F/"%(&#8%(A5(8%I%C#3%8(75A<;(WA57/C(1ccE(d:W:(-(/<8(eD` O2%(/8I/<'/;%5(#.('2%(8%I%C#3%8(@#8%C(#.(/(&#@37'%"(<%'F#"P5(5%&7"A'9(595'%@(/"%(8A5&755%84

1.1. Introduction

M7"A<;(5%I%"/C(C/5'(9%/"5('2%(&#@37'%"(<%'F#"P(/<8(A<.#"@/'A#<(5%&7"A'9(/"%('2%(3"#>C%@5(#. /(>A;(&#<&%"<(FA'2A<(A<.#"@/'A#<('%&2<#C#;9("%5%/"&2(/"%/4(?<&"%/5A<;(#.(&#@37'%"(<%'F#"P5(5&/C% /<8(A<'%<5AI%(%@%";A<;(#.(<%F(A<.#"@/'A#<('%&2<#C#;A%5E(5A;<A.A&/<'(;"#F'2(#.(&#@37'%"(<%'F#"P5 '"/..A&(/<8(#'2%"(./&'#"5(%<2/<&%('2%(<7@>%"(#.(3#55A>C%('/";%'5(.#"(/''/&P5(/;/A<5'(&#@37'%" <%'F#"P4(D/C%./&'#"5(>%&#@%(/"@%8(>9(I/"A%'9(#.(5#32A5'A&/'%8('##C5('#(>"%/P(A<('2%(5%&7"A'9 595'%@5(/5(F%CC(/5('#(2A8%(/<(#&&7""%<&%(#.(/''/&P54(:CC(/>#I%(./&'#"5(<%;/'AI%C9(A<.C7%<&%(73#<('2% %..A&A%<&9(#.('2%(%SA5'A<;(&#@37'%"(<%'F#"P5(3"#'%&'A#<(595'%@5(/<8(%</>C%(5%5/"&2(/<8 8%I%C#3@%<'(#.(<%F(3"#'%&'A#<(@#8%C5(/<8('%&2<#C#;A%5(Zf:CC%<(*et al*=LLgE(f_#"'2&7''=TTgE(f!'/&%P *et al*=T,g[4

?'(A5(F%CC(P<#F<('2/'('2%(3"#'%&'A#<('##C5(75%8(/'(3"%5%<'(%C5%F2%"%('#(3"%I%<'(/(<#<= /7'2#"A]%8(/&&%55('#('2%(&#@37'%"(<%'F#"P("%5#7"&%5(&/<(<#'(/557"%(7''%"C9(#"(%I%<(5/'A5./&'#"9('2% &#@37'%"(<%'F#"P(5%&7"A'94(:5(/<(%S/@3C%('2%(.A"%F/CC(&/<(>%(&#<5A8%"%84(:(.A"%F/CC(A5(#3%"/'%5(/5 /(>/""A%"(>%'F%%<(A<<%"(Z8%.%<8%8[(/<8(#7'%"(Z.#"(%S/@3C%E(?<'%"<%'[(&#@37'%"(<%'F#"P5(/<8(.AC'%"5 A<37'(/<8(#7'37'('"/..A&(/&&#"8A<;('#(/<(/&&%3'%8(3#CA&94(K#F%I%"E('2A5(3"#'%&'A#<(A5(<#'(/CF/95 %..A&A%<'(87%('#(@/<9("%/5#<5E(.#"(%S/@3C%E(87%('#(.#CC#FA<;(#<%5(fV/&%=TTE(:CC%<(*et al*=LLgB

- Z*[(:(3/"'(#.('2%(A<37'(/<8(#7'37'('"/..A&(&/<(>93/55('2%(.A"%F/CCE(>%&/75%(75%"5(5#@%'A@%5 %5'/>CA52(7</7'2#"A]%8(&#<<%&'A#<5(FA'2(#7'%"(&#@37'%"(<%'F#"P54
- Z-[(O2%(@#5'(3/"'(#.('2%(<%'F#"P(5%&7"A'9(8/<;%"5(3"#&%%85(."#@('2%(/7'2#"A]%8(75%"5(F#"PA<; A<5A8%('2%(`:_(/5(F%CC(/5(."#@('2%(>7;5(%@>%88%8(A<'#(5#.'F/"%(/<8a#"(2/"8F/"%4
- Z0[(YA"%F/CC('2%@5%CI%5(&/<(>%(/('/";%'(#.('2%(57&&%55.7C(/''/&P5(>%&/75%(/(.A"%F/CC(75%5 I7C<%"/>C%(<%'F#"P(#3%"/'A#<(595'%@(/<8(75%5(/("%/CA]/'A#<(#.('2%(O1!a?!(5'/&P(3"#'#&#CE F2A&2(A5(I7C<%"/>C%(A<('7"<4
- ZG[(O2%"%(%SA5'(/(<7@>%"(#.(/''/&P5('2/'(/"%(&/3/>C%('#(>93/55('2%(.A"%F/CC4(Y#"(%S/@3C%E(57&2 /''/&P5(&/<(75%('2%(5#=&/CC%8(\'7<<%C=@#8%\(/''/&P('2/'(%@3C#95(/(>C#&P%8(.A"%F/CC(3"#'#&#C 5A'7/'%8(A<5A8%('2%(A<37'('"/..A&(ZA<37'(@%55/;%[4

O2#5%(/"%('2%("%/5#<5(F29(A'(A5(<#'(3#55A>C%('#(3"%I%<'(&#@3C%'%C9(57&&%55.7C(/''%@3'5(#. <#<=/7'2#"A]%8(/&&%55('#('2%(8A5'"A>7'%8(A<.#"@/'A#<("%5#7"&%5(#.(&#@37'%"(<%'F#"P54(O2%(C/''%"(A5

'2%("%/5#<(F29(A<('2%(&#@37'%"(<%'F#"P(5%&7"A'9(/"%/('2%('#3=2#'('/5P(A5(@#<A'#"A<;(#.('2%(A<37' '"/..A&(/<8(F%CC='A@%8(8%'%&'A#<(#.(/''/&P5('#(8%&"%/5%('2%(3#55A>C%(<%;/'AI%(%..%&'54

O2%("%&%<'(5%&7"A'9(@#8%C5(.#&75(#<(/<(A8%/(#.(&##3%"/'A#<(#.('2%(8A5'"A>7'%8(<%'F#"P 5%&7"A'9(&#@3#<%<'5(5A'7/'%8(>#'2(A<5A8%(/<8(#7'5A8%(#.(/(3/"'A&7C/"(<%'F#"P(2#5'4(: C#<;(FA'2 &#<I%<'A#</CC9(75%8(5%&7"A'9('##C5(CAP%(.A"%F/CCE(/&&%55(&#<'"#CE(/7'2%<'A&/'A#<(/<8(A8%<'A.A&/'A#< 595'%@5E(A<'"75A#<(8%'%&'A#<(595'%@5(Z?M6[(/"%(>%&#@A<;(#.(;"%/'(5A;<A.A&/<&%4

?M6(A5(/(&#@3#<%<'(#.(/(5%&7"A'9(595'%@(&#CC%&'A<;(A<.#"@/'A#<(."#@(8A..%"%<'(%<'"9(3#A<'5(#. /(&#@37'%"(<%'F#"P(>%A<;(3"#'%&'%8E(/<8(/</C9]A<;('2%(&#CC%&'%8(A<.#"@/'A#<('#(8%'%&'(.%/'7"%5(/<8 ./&'5(>#'2(#.(/(5753A&A#75(75%"(>%2/IA#"(ZA<'%"3"%'%8(/5(/''%@3'5(#.(A<'"75A#<[(/<8(A<'"75A#<5(/A@%8 /'(&#@3"#@A5A<;('2%(<%'F#"P(5%&7"A'94

?M6(3%".#"@/<&%(A5(>/5%8(#<('2%(A<37'('"/..A&(@#<A'#"A<;4(^ 2AC%(@#<A'#"A<;('2%(A<37'('"/..A&E ?M6(8%'%&'5(%I%<'5E(3/''%"<5(&#<5A5'A<;(#.('2%(3"%8%.A<%8(5%U7%<&%5(#.(%I%<'54(O2%(8%'%&'%8(3/''%"<5 .#"@(A<37'(./&'5(#.(P<#FC%8;%=>/5%8(&#@3#<%<'5(#.(?M6("%53#<5A>C%(.#"('2%(A<'"75A#<(8%'%&'A#<4 O2%5%(&#@3#<%<'5(@/P%(8%&A5A#<5(#<('2%(>/5A5(#.("7C%5E(F2#5%('"7'2=I/C7%5(8%3%<8(#<(A<37'(./&'5 Z8%'%&'%8(3/''%"<5[4(h5A<;(?M6(/CC#F5('#(A@3"#I%(A<'%;"A'9(/<8(%..A&A%<&9(#.('2%(5%&7"A'9(595'%@(/5 /(F2#C%E(#<=CA<%(@#<A'#"A<;(#.(75%"5i(/&'AIA'9E("%&#;<A'A#<(#.E(<#'A.A&/'A#<(/>#7'(/<8E(3#55A>C9E .ASA<;(&#""73'%8(595'%@(.AC%5(/<8(8/'/(/5(F%CC(/5(595'%@(&#<.A;7"/'A#<(/C'%"A<;E(%'&4(fV/&%=TTE(:CC%< *et al*=LLE(:S%C55#<=LLE(_#"'2&7''=TTg4

O2%(@#5'(P<#F<("%3"%5%<'/'AI%5(#.(%S3C#"/'#"9(?M6E(F2A&2(&#<'"A>7'%8(3A#<%%"(5#C7'A#<5('# '2%(A<.#"@/'A#<(5%&7"A'9(.A%C8E(/"%(K/95'/&P(Zf6@/2/=,,g[E(D?M:6(Zf6%>"A<; *et al*=,,g[E(?MR6 Zf`7<' *et al*=,,g[E(_:M?J(Zfd/&P5#<(*et al*=T*g[E(M?M6(Zf6</33 *et al*=T-g[E(:6:e(ZfK/>"/ *et al*=T-g[E h6O:O(Zf?C;7<=T0g[E(?M?HO(Zfb7@/" *et al*=TGg[E(_?MR6(Zf:<8%"5#< *et al*=TNg[E(X"?M6(Zf6'/<A.#"8 12%<=T+g[E(d/<75(ZfX#C8>%";(*et al*=T+g[E(dA_/#(Zfd#7 *et al*=TQg[E(RDRJ:`M(Zf!#""/5 *et al*=TQg[E _%'6O:O(ZfWA;</(*et al*=T,g[E(V"#(Zf!/S#<=T,g[E(!=VR6O(Zf`A<8UIA5' *et al*=TTg[E(%'&4

O2%(@/A<(8A5/8I/<'/;%5(#.('2%(&7""%<'C9(%SA5'A<;(&#@@%"&A/C(/<8(@/$#"A'9(#.('2%("%5%/"&2 ?M6(/"%(/5(.#CC#F5(Zf:CC%<(*et al*=LLgE(f:S%C55#<=LLgE(f`A33@/<<(*et al*=T,gE(f!'/&%P(*et al*=T,gE fV/C/57>"/@/<A9/<(*et al*=T,gE(fj/<; *et al*=LLgE(fX#"#8%'5PA-(*et al*=LLg[B

Z*[('##(2A;2(3"#>/>ACA'9(#.(./C5%(3#5A'AI%5(/<8(./C5%(<%;/'AI%5k

Z-[(F%/P(/>ACA'9(A<(8%'%&'A#<(#.(<%F(3"%IA#75C9(7<P<#F<('93%5(#.(/''/&P5k

Z6g[T6c(30.()-0-2/4922(A&2(1)5(63T)A<-8(6(9)58.61%.6.(6.(6)85(@/639.(A<'2.1(#(/63(A<()-248%0012T)-(/63(A</3.2(.8(A1!6CA'8(A1!60

5A@3CA.A%8(I%"5A#<(#.(/;%<'5n(/"&2A'%&'7"%(/<8('2%A"(&##3%"/'AI%(>%2/IA#"(/<8(8#(<#'(%@3C#9('2% &/3/>ACA'A%5(#.(@7C'A=/;%<'('%&2<#C#;94(?<(3/"'A&7C/"E('2%(3"#3#5%8(@#8%C5(/<8(/"&2A'%&'7"%5(75% /;%<'5(/'('2%(3"%=3"#&%55A<;(32/5%(#.('2%(3"#'%&'A#<('/5P4(K%"%('2%(/;%<'5(/"%(<#'(P<#FC%8;%=>/5%8E /"%(@/</;%8(>9(/(2A;2=C%I%C(5#.'F/"%(@/</;%"E("%5'"A&'%8(>9(5#CIA<;(A<'"75A#<(8%'%&'A#<('/5P(/<8(8# <#'(A<'%"/&'(FA'2('2%(/&&%55(&#<'"#C(/<8(#'2%"(5%&7"A'9(595'%@(&#@3#<%<'54(?<(./&'E('2%9(8#(<#'(75%(/ 5%&7"A'9(&#@3#<%<'(&##3%"/'A#<('2/'(&/<(3"#IA8%(.#"(/(@#5'(5A;<A.A&/<'(&#<'"A>7'A#<(/(U7/CA'9(#. &#@37'%"(<%'F#"P(3"#'%&'A#<4

O2%(&2/3'%"(A5(.#&75%8(#<('2%(/"&2A'%&'7"%(/<8(A@3C%@%<'/'A#<(#.(/(&/5%(5'789(/A@A<;(/'('2% %S3C#"/'A#<(#.(3#'%<'A/C(/8I/<'/;%5(#.(@7C'A=/;%<'(/"&2A'%&'7"%(.#"('2%(&#@37'%"(<%'F#"P(3"#'%&'A#< ZfX#"#8%'5PA*(*et al*=LLgE(fX#"#8%'5PA-(*et al*=LLg[4(?'(8%5&"A>%5('2%(&#<&%3'7/C(@#8%C(/<8(/"&2A'%&'7"% #.(3/"'A&7C/"(53%&A/CA]%8(/;%<'5(/<8('2%(595'%@(#<(/(F2#C%E('2%(A@3C%@%<'/'A#<('%&2<#C#;9(/5(F%CC /5('2%(5A@7C/'A#<(3"#&%87"%(/<8(5#@%(#.(A'5("%57C'54(O2%(@/$#"(/''%<'A#<(A5(3/A8('#('2%(A<'"75A#< 8%'%&'A#<('/5P(/<8(/;%<'5(A<'%"/&'A#<5(87"A<;(8%'%&'A#<(#.(/<(/''/&P(/;/A<5'('2%(&#@37'%"(<%'F#"P4

O2%("%5'(#.('2%(12/3'%"(A5(5'"7&'7"%8(/5(.#CC#F54(*Section 1.2*(;AI%5(/<(#I%"IA%F(#.('2%("%57C'5 #.('2%(!"#$%&'("%5%/"&2(#>'/A<%8(/'('2%(3"%IA#75(32/5%5(/<8('2%A"(A<'%"&#<<%&'A#<(FA'2('2%("%57C'5 8%5&"A>%8(>%C#F(A<('2A5(12/3'%"4(*Section 1.3*(8%5&"A>%5('2%(2A;2=C%I%C(/"&2A'%&'7"%(#.('2%(8%I%C#3%8 @7C'A=/;%<'(5%&7"A'9(595'%@E(F2A&2(A<'%;"/'%5(8A5'"A>7'%8(2#5'=>/5%8(@7C'A=/;%<'(5%&7"A'9(595'%@54 O2%(/"&2A'%&'7"%(#.('2%(3/"'A&7C/"(2#5'=>/5%8(5%&7"A'9(595'%@(A@3C%@%<'%8(/5('2%(&/5%(5'789(A5 &#<5A8%"%8(A<(*Section 1.4*4(*Section 1.5*(8%5&"A>%5('2%(/"&2A'%&'7"%(#.(/(3/"'A&7C/"(5%&7"A'9(/;%<'4(: @#8%C(#.('2%(%S'%"</C(%<IA"#<@%<'(#.('2%(&/5%(5'789(A@3C%@%<'%8(/5(\?<37'(O"/..A&(D#8%C\ @#8%CA<;(/(@7C'A'78%(#.(8A5'"A>7'%8(/''/&P5(A5(8%5&"A>%8(52#"'C9(A<(*Section 1.6*.(*Section 1.7*(;AI%5 >"A%.(A<.#"@/'A#<(/>#7'('2%('%&2<#C#;9(75%8(.#"(@#8%CA<;(/<8(A@3C%@%<'/'A#<(#.('2%(1/5%(6'7894 1/5%(6'789(5A@7C/'A#<(3"#&%87"%(A5(8%5&"A>%8(A<(*Section 1.8*4(?<(3/"'A&7C/"E(A<('2A5(5%&'A#<(/< %S/@3C%(#.(/(8A5'"A>7'%8(/''/&P(/<8(#3%"/'A#<(#.('2%(&/5%(5'789(/5(/("%/&'A#<('#(/(3/"'A&7C/" 8A5'"A>7'%8(/''/&P(/;/A<5'(&#@37'%"(<%'F#"P('#(>%(3"#'%&'%8(A5(;AI%<4(*Section1.9*(3"%5%<'5('2% &#<&C75A#<E(F2A&2(57@@/"A]%5('2%("%57C'5(&#<&%"<A<;(/(;%<%"/C(/55%55@%<'(#.('2%(8%I%C#3%8(&/5% 5'789(/<8(3#'%<'A/C(/8I/<'/;%5(#.(75A<;(@7C'A=/;%<'(/"&2A'%&'7"%(.#"(&#@37'%"(<%'F#"P(5%&7"A'9 595'%@4

1.2. Overview of the Results Presented in Previous Reports

1#<'%@3#"/"9(IA%F(#<('2%(3"#>C%@(#.(A<.#"@/'A#<(5%&7"A'9(A5(&#<&%"<%8(FA'2(/<(A8%/('2/' 3/"'A&7C/"(3"#'%&'AI%(@%&2/<A5@5(/<8(&#""%53#<8A<;(5#.'F/"%(@75'(>%(A<'%;"/'%8(A<'#(/(8A5'"A>7'%8 595'%@(#.('2%(/7'#<#@#75(5#.'F/"%(%<'A'A%5(A<'%"/&'A<;(IA/(@%55/;%(%S&2/<;%(/<8(@/PA<;(8%&A5A#<5 A<(/(&##3%"/'AI%(/<8(&##"8A</'%8(@/<<%"4(O2%5%(5#.'F/"%(%<'A'A%5(52#7C8(>%(/8/3'AI%('#(<%'F#"P '"/..A&(I/"A/'A#<5E('#("%&#<.A;7"/'A#<(#.('2%(<%'F#"P(5#.'F/"%(/<8(2/"8F/"%(&#@3#<%<'5(/<8('# 7<P<#F<('93%5(#.(/''/&P4(H<%(#.('2%(*objectives of this Project*(A5(%S3C#"/'A#<(#.('2%(@7C'A=/;%<' '%&2<#C#;9(/5('2%(."/@%F#"P(.#"(@#8%CA<;(/<8(A@3C%@%<'/'A#<(#.(&#@37'%"(<%'F#"P(5%&7"A'9 595'%@5(/<8(A'5(/>ACA'A%5('#(@%%'('2%(/.#"%@%<'A#<%8("%U7A"%@%<'54

:&&#"8A<;('#('2%(^#"P(!"#;"/@('2%(!"#$%&'("%5%/"&2(F/5(&/""9A<;(#7'(A<(5%I%"/C(32/5%5(/<8 "%57C'5(#.(%/&2(5'/;%(F%"%(57>@A''%8(A<('2"%%(?<'%"A@(J%3#"'5(/<8(A<(YA</C(J%3#"'()*4(O2A5("%3#"'(A5 &#<&C78A<;(#<%4(O2A5(J%3#"'(3"%5%<'5(.A</C("%57C'5E(F2A&2(/"%(/(</'7"/C(&#<'A<7/'A#<(/<8(#>I%"5% FA'2("%;/"8('#('2%(3"%IA#75("%57C'54(`%'(75(;AI%(/(>"A%.(57@@/"9(#.('2%("%57C'5(3"%5%<'%8(A<(3"%IA#75 "%3#"'5('#("%@A<8(/>#7'('2%@E('#(&#<<%&'('2%@(FA'2('2%("%57C'5(3"%5%<'%8(A<('2A5(#<%E(/<8('#(@/P% /I/AC/>C%('2%(&#@3C%'%(7<8%"5'/<8A<;(#.('2%("%57C'5(#<('2%(F2#C%4

?<(*the Interim Report #1*(f?<'J%3)*g('2%(.#CC#FA<;('/5P5(F%"%('2%(57>$%&'5(#.('2%("%5%/"&2B

Z*[(#I%"IA%FE(/</C95A5(/<8(&C/55A.A&/'A#<(#.('2%('2"%/'5(/<8(3#55A>C%(/''/&P5(#<(&#@37'%" <%'F#"Pk

Z-[(/CC#&/'A#<('/5P5(#I%"(3/"'A&7C/"(/;%<'5(#.('2%(&#@37'%"(<%'F#"P(5%&7"A'9(595'%@(Z1_66[k

Z0[(8%I%C#3@%<'(#.('2%(/;%<'(&#@@7<A&/'AI%(3"#&%87"%54

?<(5#@%(5%<5%E('2%("%57C'5(#.(*first task*(@/8%(A'(3#55A>C%('#(7<8%"5'/<8('2%(%<IA"#<@%<'(FA'2A< F2A&2(/(@#8%"<(&#@37'%"(<%'F#"P(A5(#3%"/'A<;E(3#'%<'A/C(A<5A8%(/<8(#7'5A8%(/''/&P5E(8%;"%%5(#.('2% 3/"'A&7C/"(/''/&P(8/<;%"(A<("%53%&'('#('2%(3#55A>C%(/.'%"..%&'5E(/<8(8%;"%%(#.('2%(<%'F#"P

I7C<%"/>ACA'94(O2A5(@/'%"A/C(.#"@%8(/(5'/'"A<;(3#A<'(.#"(.7"'2%"(%..#"'5(A<(8%I%C#3@%<'(/<(/;%<'= >/5%8(@#8%C(#.(1_664(D/A<(&#<&%3'5(#.("%@#'%(/''/&P5(#<(&#@37'%"(<%'F#"P5(F%"%(&#<5A8%"%84 O2%(5'/<8/"8("%@#'%(/''/&P(A5('2%("%@#'%(7</7'2#"A]%8(A<.#"@/'A#<(%..%&'E("%/CA]%8(#<(8/'/(CA<P5 '2/'(A5('93A&/C('#(/<9(&#@37'%"(<%'F#"P4(O2%(37"3#5%5(#.('2%(3"#$%&'(&/75%8(/(<%&%55A'9(#. %C/>#"/'A#<(#.('2%(5/'A5./&'#"9(&#@37'%"(/<8(<%'F#"P(/''/&P('/S#<#@A%5(/<8(/(@7C'A.#C8 &C/55A.A&/'A#<(#.('2%("%@#'%(/''/&P54(M7"A<;('2%(.A"5'(32/5%("%5%/"&2(&2/"/&'%"A5'A&5(#.(5/'A5./&'#"9 '/S#<#@A%5(#.(/''/&P5(F%"%(/</C9]%8(/<8(/("%IA%F(#.('2%(%SA5'A<;(/''/&P(/;/A<5'(5A<;C%(&#@37'%" /<8(/;/A<5'(&#@37'%"(<%'F#"P('/S#<#@A%5(F/5(3"%5%<'%84(O2%(C/'%"(A<&C78%8(/(CA5'(#.(/''/&P("%"@5E /(CA5'(#.(/''/&P(&/'%;#"A%5E(/''/&P("%57C'5(&/'%;#"A%5E(%@3A"A&/C(CA5'5(#.(/''/&P('93%5E(I7C<%"/>ACA'A%5 @/'"A&%5E(/&'A#<=>/5%8('/S#<#@A%5E(5%&7"A'9(.C/F5(#"(I7C<%"/>ACA'A%5('/S#<#@A%5E(/(&C/55A.A&/'A#<(#. A<'"75A#<5(>/5%8(#<('2%(5A;</'7"%5E(/<8(A<&A8%<'('/S#<#@A%5(Z'2%(5%&7"A'9('%"@A<#C#;9(#.(&#@@#< C/<;7/;%(.#"(5%&7"A'9(A<&A8%<'5(/"%(&#<5A8%"%8(2%"%[4(?'(F/5(&#<&C78%8('2/'('2%(A<&A8%<'('/S#<#@A%5 /"%('2%(@#5'(3"#@A<%<'(.#"(!"#$%&'(;#/C5E(>7'('2%9("%U7A"%(/(8%%3%"(/</C95A5(FA'2(%@32/5A5(#< "%@#'%(/&'A#<54(O2A5(3/"'(#.('2%("%5%/"&2("%57C'%8(A<('2%(8%I%C#3@%<'(#.('2%(&C/55A.A&/'A#<(#. 5'/<8/"8("%@#'%(/''/&P54(?<('2A5(&C/55A.A&/'A#<(%/&2(/''/&P(53%&A.A%5(>9('2%(A<'%<8%8(%..%&'E(37"3#5% #.('2%(/''/&PE(&#<8A'A#<5(3"#IA8A<;(.#"('2%(%..%&'(/&2A%I%@%<'E(%SA5'%<&%(#.(/(.%%8>/&P(FA'2('2% /''/&P%8(#>$%&'E(C/9#7'(#.('2%(57>$%&'(#.(/''/&P(&#<&%"<A<;('2%(/''/&P%8(#>$%&'E(C/9%"(#.(5'/<8/"8 ?6HaH6?(@#8%C(#<(F2A&2('2%(%..%&'(A5(&/"A%8(#7'E '2%(#>$%&'('2/'(A5('2%(/''/&P('/";%'4(V%5A8%5E '93A&/C(5&2%@%5(#.('2%("%@#'%(/''/&P5(@/33%8('#('2%(8%I%C#3%8(&C/55A.A&/'A#<(F%"%(A<'"#87&%84(?' F/5(8%5&"A>%8(5AS(;%<%"A&(5&2%@%5(#.('2%("%@#'%(/''/&P5('2/'(/"%(/5(.#CC#F5B

- /</C95A5(#.('2%(<%'F#"P('"/..A&(Z#"(CA5'%<A<;(#.(/(8/'/(CA<P(>9(@%/<5(#.(53%&A/C('##C5(o 5<A..%"5[E
- <%'F#"P(5&/<<A<;E
- 57>5'A'7'A#<(#.('2%('"75'%8(#>$%&'(#.('2%(<%'F#"P(/<8('"/<5@A55A#<(#<(8/'/(CA<P5(#.('2% @%55/;%5(."#@(A'5(</@%(FA'2(/33"#3"A/'A#<(#.(A'5(/&&%55("A;2'5E
- A@3C/<'/'A#<(#.('2%(./C5%(#>$%&'(#.('2%(<%'F#"PE
- 8%<A/C(#.(5%"IA&%E
- "%@#'%(%S%&7'A#<(#.(/33CA&/'A#<54

: &&#"8A<;('#('2%(*second task*(#.('2%(.A"5'(32/5%("%5%/"&2('2%(/;%<'=>/5%8(/"&2A'%&'7"%(#. 1_66(F/5(8%I%C#3%8(&#<&%3'7/CC94(:5(F%CCE('2%(/"&2A'%&'7"%5(#.('2%(3/"'A&7C/"(5#.'F/"%(/;%<'5(/<8 /CC#&/'A#<(3/"'A&7C/"('/5P5(#I%"('2%@(F%"%(&/"'"A%8(#7'4(H<%(#.('2%("%57C'5(#.('2A5(32/5%(F/5('2% 8%I%C#3@%<'(#.('2%(;%<%"/C(."/@%F#"P(.#"(8A5'"A>7'%8("%3"%5%<'/'A#<(#.('2%(5%&7"A'9(595'%@ P<#FC%8;%('2/'(@/P%5(3#55A>C%('#(5733#"'(/;%<'(&##3%"/'A#<(/<8('2%A"(@7'7/C(7<8%"5'/<8A<;4(O2% >/5A5(#.('2A5(."/@%F#"P(A5(57>$%&'(8#@/A<(#<'#C#;94

O2%(3"#3#5%8(/"&2A'%&'7"%(&#@3"A5%5(/(<7@>%"(#.(53%&A/CA]%8(&##3%"/'A<;(5%&7"A'9(/;%<'54 O2%(5%'(#.(/;%<'5(A<&C78%5

- *Intrusion detection agents*("%53#<5A>C%(.#"(8%'%&'A#<(A<'"75A#<(#<('2%(>/5A5(#.(A<.#"@/'A#< "%&%AI%8(."#@(#'2%"(/;%<'5(/>#7'(3#55A>C%(/<#@/CA%5E(5753A&A#75(>%2/IA#"(#.(75%"5E(/''%@3'5 #.(<#<=/7'2#"A]%8(/&&%55(%'&4
- *Access control agents*(3"#IA8A<;(/<(/&&%55('#('2%(A<.#"@/'A#<("%5#7"&%5(A<(/&&#"8/<&%(FA'2 '2%(75%"5n(/7'2#"A'94
- *Identification and authentication agents*("%53#<5A>C%(.#"(A8%<'A.A&/'A#<(#.(A<.#"@/'A#< 5#7"&%5(/<8(&#<.A"@/'A#<(#.('2%A"(/7'2%<'A&A'94

O2%5%(/;%<'5(F%"%(&#<5A8%"%8(/5(>/5A&(#<%5(A<('2%(.7'7"%(8%I%C#3@%<'(#.('2%(@7C'A=/;%<' 1_66(/"&2A'%&'7"%(/<8(A'5(5#.'F/"%(A@3C%@%<'/'A#<4(?<(;%<%"/C(&/5%E(A'(A5(@/P%(5%<5%('#(%S'%<8('2% /"&2A'%&'7"%('2"#7;2(A<&C78A<;(5#.'F/"%(/;%<'(#.(#'2%"(PA<8('2/'(/"%

- *Attack suppression agents*("%/CA]A<;(p3"#5%&7'A#<q(/<8(<%7'"/CA]/'A#<(#.('2%(/''/&PA<;(3"#;"/@5 ZA<'"78%"5[E
- *Agents of damage assess*(/<8(A<.#"@/'A#<(A<'%;"A'9("%&#I%"9("%53#<5A>C%(.#"(A<.#"@/'A#< A<'%;"A'9(%<57"A<;E
- *Cryptography and steganography*(3"#'%&'A#<(/;%<'5(75%8(.#"(&"%/'A#<(#.(5/.%=%S&2/<;% &2/<<%C5(>%'F%%<(<%'F#"P(<#8%5(Z2#5'5E(5%"I%"5[E

- *Learning agents*("%53#<5A>C%(.#"(/8/3'/'A#<(#.(1_66(/;%<'5('#(&#@37'%"(<%'F#"P "%&#<.A;7"/'A#<(/<8(/''/&P5(#.(<%F('93%54

?<(5#@%(&/5%5(A'(&/<(>%("%/5#</>C%('#(A<&C78%(A<(/"&2A'%&'7"%(/(5#=&/CC%8(@%'/=/;%<' "%53#<5A>C%(.#"(@/</;A<;('2%(A<.#"@/'A#<(5%&7"A'9(3"#&%55%E(3"#I A8A<;(.#"(&##3%"/'%8(>%2/ IA#"(#. '2%(5%&7"A'9(/;%<'5(/<8("%/CA]A<;('2%("%U7A"%8(C%I%C(#.(;%<%"/C(5%&7"A'9(A<(/&&#"8/<&%(FA'2(/(;C#>/C &"A'%"A#<4

O2%(*third task*(F/5(8%I#'%8('#('2%(8%I%C#3@%<'(#.('2%(/;%<'i5(&#@@7<A&/'A#<(/"&2A'%&'7"%E F2A&2(A5('2%(P%9(&#@3#<%<'(#.(%I%"9(@7C'A=/;%<'(595'%@(>%&/75%('2%(3%".#"@/<&%(#.(%/&2(/;%<'(A5 A<'A'/'%8(>9(5'"%/@(#.(A<37'(@%55/;%54(O#(53%&A.9('2%(@%55/;%5E(/;%<'(&#@@7<A&/'A#<(C/<;7/;% bmD`(F/5(&2#5%<(.#"(75%4(bmD`(69<'/S(ZFA'2(/(5%'(#.(/88A'A#</C(/33CA&/'A#<=#"A%<'%8(P%9F#"85[F/5(53%&A.A%84(O#(53%&A.9(/(@%55/;%(&#<'%<'(A'(A5(5733#5%8(/'('2A5(32/5%('#(75%(b?Y(C/<;7/;%4(`/'%" '2A5(8%&A5A#<(F/5(&2/<;%8(A<(./I#"(#.(eD`(C/<;7/;%4

O2%(57>$%&'5(#.('2%(*Interim Report #2*(f?<'J%3)-g(F%"%('2%("%57C'5(#.("%5%/"&2(#<('2% .#CC#FA<;('/5P5B(Z*[(8%I%C#3@%<'(#.('2%(@#8%C5(#.(8A5'"A>7'%8(&#@@#<(/<8(53%&A.A&(P<#FC%8;%(#. /;%<'5E(Z-[(#>$%&'=#"A%<'%8(8%5A;<(#.('2%(5#.'F/"%('##C(3"#'#'93%(#.(/;%<'=>/5%8(1_66(/<8(Z0[8%I%C#3@%<'(#.('2%(3/"'A&7C/"(5#.'F/"%(&#@3#<%<'54

O2%(*first task*(F/5(.#&75%8(#<('2%(#<'#C#;9=>/5%8("%3"%5%<'/'A#<(#.(8A5'"A>7'%8(&#@@#<(/<8 53%&A.A&(P<#FC%8;%(#.(/;%<'5(#.('2%(@7C'A=/;%<'(A<.#"@/'A#<(5%&7"A'9(595'%@4(O2%("%57C'5(#. "%5%/"&2(#<('2%(.A"5'('/5P(F%"%(53%&A.A&/'A#<(#.('2%(1_66(&#<&%3'7/C(@#8%CE(3"A<&A3C%5(#.(75A<; #<'#C#;9(.#"(5'"7&'7"A<;(#.('2%(5%&7"A'9(/;%<'5n(P<#FC%8;%(/5(F%CC(/5(/</C95A5(#.('2%(#<'#C#;9(/5(/ ."/@%F#"P(.#"(8A5'"A>7'%8(P<#FC%8;%("%3"%5%<'/'A#<4

1_66(&*onceptual model* F/5(53%&A.A%8(/5(/(@7C'A'78%(#.(5%&7"A'9(/;%<'5('2/'(/"%(/7'#<#@#75 3"#;"/@5(8A5'"A>7'%8(#I%"('2%(<%'F#"P(2#5'5E(5#CI A<;(/CC#&/'%8(5%&7"A'9('/5P5(/<8(A<'%"/&'A<;(/@#<; %/&2(#'2%"(.#"(&##3%"/'A#<4(O2%(>/5A&(/;%<'5(#.(/(2#5'(/"%(/;%<'=8%@#<5(A<'%<8%8('#(3"%3"#&%55('2% A<37'('"/..A&E(A8%<'A.A&/'A#<(/<8(/7'2%<'A&/'A#<(/;%<'E(/&&%55(&#<'"#C(/;%<'E(A<'"75A#<(8%'%&'A#< /;%<'5E(/<8(@%'/=/;%<'5(#.(/(2#5'4(_#'A&%('2/'(C/'%"(A'(F/5(8%&A8%8('#("%.75%(."#@('2%(A<&C78A<;(A< '2%(2#5'(>/5%8(5%&7"A'9(595'%@(/(@%'/=/;%<'(/<8('#(#";/<A]%('2%(/;%<'(&##3%"/'A#<(A<(/(37"% 8A5'"A>7'%8(F/94(O2A5(A8%/(F/5(A@3C%@%<'%8(C/'%"(A<('2%(1/5%(6'789(5#.'F/"%4

:(.7"'2%"(/"%<'A#<(F/5(3/A8('#('2%(8%I%C#3@%<'(#. '2%(8#@/A< *ontology* /5(/(.#"@/C ."/@%F#"P(.#"(5'"7&'7"A<;(8A5'"A>7'%8(P<#FC%8;%(>/5%4(O2%(3"#3#5%8(*ontology-based framework* .#"(8%I%C#3@%<'(/<8("%3"%5%<'/'A#<(#.('2%(1_66(8A5'"A>7'%8(P<#FC%8;%(F/5(A<'%<8%8('#(3"#I A8%(.#" @/A<'%</<&%(#.(/;%<'5n(P<#FC%8;%(A<'%;"A'9E(&#<5A5'%<'(@#8A.A&/'A#<(#.('2%(3/"'A&7C/"(/;%<'5n P<#FC%8;%E(&#<5A5'%<'(/;%<'(&C#<A<;E(%'&4(?'(F/5(75%8(/5(/(>/5A5(#.('2%(@%'2#8#C#;9(#.('2%(1_66 #>$%&'(#"A%<'%8(8%5A;<4

The most significant "dimensions" of the entire ontology of the security concepts and tasks F%"%("%3"%5%<'%8(>9('2%(p5%&7"A'9(/;%<'5(8#@/A<qE(p@%55/;%=%I%<'=/'"/&P(3"#&%55A<;qE(p5A<;C% /''/&P('93%5qE(p5A<A.A&/<'(%I%<'5qE(p5%&7"A'9(/;%<'5o(/''/&P(&C/55%5o(5A;<A.A&/<'(%I%<'5qE(p5%&7"A'9 /;%<'5n(#3%"/'A#<5q(/<8(p5&%</"A#5(#.(/''/&P5o(5%&7"A'9(/;%<'(&##3%"/'A#<q(&#@3#<%<'54

The "security agents' domain" ontology 5%'5(3/"'A&7C/"(.7<&'A#</CA'9(/<8(/"%/(#. "%53#<5A>ACA'9('#(%/&2(3/"'A&7C/"(5%&7"A'9(/;%<'4(?'(;#I%"<5('2%(%<'A"%(8%I%C#3@%<'(&9&C%(#.('2% 1_66(&#@3#<%<'54

The "message-event-attack processing" ontology 53%&A.A%5(3"#&%55A<;(#.(@%55/;%5(."#@ C#F%"('#(733%"(C%I%C5(#.(;%<%"/CA]/'A#<(/<8(&C/55A.A&/'A#<4(O2%(3/"'A/CC9(#"8%"%8(5%'(#.(>/5A& &#<&%3'5(A<&C78%5(@%55/;%('"/..A&E(%I%<'E(5A;<A.A&/<'(%I%<'E(&"A'A&/C(%I%<'E(/78A'("%&#"8E(3/''%"<E "7C%5E(/&'A I A'9E(5&%</"A#(#.(/&'A I A'9E(&#<<%&'A#<E(5A@3C%(Z\5A<;C%=32/5%[(/''/&PE(&#@3#5A'%(Z\@7C'A= 32/5%\[(/''/&P4(*The "single attack types" ontology* 53%&A.A%5(5A<;C%=32/5%(/''/&P5E(#"8%"%5(&C/55%5(#. 2#5'=>/5%8(/<8(<%'F#"P=>/5%8(&#@3#<%<'5(#.(/''/&P54(O2%(%A;2'('93A&/C(*classes of single phase attacks* 5%C%&'%8(.#"(5A@7C/'A#<(#.(1_66(3"#'#'%&'A#<(3%".#"@/<&%(/"%(/</C95A5(#.('2%(<%'F#"P('"/..A& Z5<A..A<;[E(<%'F#"P(5&/<<A<;(Z3"#>A<;[E(57>5'A'7'A#<(#.('2%('"75'%8(#>$%&'(#.('2%(<%'F#"PE A@3C/<'/'A#<(#.('2%(./C5%(#>$%&'(A<'#('2%(<%'F#"PE(8%<A/C(#.(5%"I A&%E(7</7'2#"A]%8(/&&%55(."#@(/ "%@#'%(@/&2A<%(>9(;7%55A<;(3/55F#"8E(7</7'2#"A]%8(/&&%55('#(C#&/C("##'(3"A IAC%;%5E("%@#'% A<A'A/'A#<(#.(/33CA&/'A#<54

The "significant events" ontology 8%.A<%5(/(2A%"/"&29(#.(%I%<'(3"#&%55A<;(C%I%C5E(/33"#3"A/'% <%'F#"P(3"#'#&#C5(/<8(5%"IA&%5E(#3%"/'A<;(595'%@(&#@@/<85(/<8(/33CA&/'A#<54(?'(3C/95(/<(A@3#"'/<' "#C%(A<("%53%&'('#(@7C'A=C%I%C(8/'/(3"#&%55A<;(3%".#"@%8(>9(5%&7"A'9(/;%<'54

The "security agents – attack classes – significant events" ontology 53%&A.A%5('2%(/"%/(#. "%53#<5A>ACA'9(#.(%/&2(3/"'A&7C/"(A<'"75A#<(8%'%&'A#<(/;%<'4(?'(8%.A<%5(/(2A%"/"&29(#.(%I%<'(3"#&%55A<; C%I%C5(@/33%8(A<'#(?M : 5n(&C/55%54

The "security agents' operations" (ordering and timing of data processing) ontology 8%'%"@A<%5(2#F('2%(5%&7"A'9(/;%<'5(52#7C8(#3%"/'%('#(8%'%&'(/''/&P5E('#(3"#'%&'(/;/A<5'(/<8('# "%53#<8('#('2%@4(O2A5(#<'#C#;9(5%'5('2%(/33"#3"A/'%(P<#FC%8;%(>/5%5E(&#<&%3'("%.%"%<&%5E(/<8 2A%"/"&29(#.(>/5%(&#<&%3'5E(5%&7"A'9('/5P5E(/5(F%CC(/5(8/'/(/<8("%57C'5(.#"@/'54

The "scenarios of attacks – security agent cooperation" ontology 53%&A.A%5(&#@3#5A'%(2#5'= >/5%8(/<8(<%'F#"P=>/5%8(8A5'"A>7'%8(/''/&P5(@/33%8(A<'#(5&%</"A#5(#.(A<'%"/&'A#<5(/<8(&##3%"/'A#< #.('2%(5%&7"A'9(/;%<'54(O2%(8%5&"A>%8(p8A@%<5A#<5q(#.('2%(%<'A"%(#<'#C#;9("%.C%&'('2%(/7'2#"5(IA%F(/' /(&#@3C%SA'9(#.('2%(1_66(@#8%C(/<8("%53%&'AI%(5#.'F/"%(3"#'#'93%('2/'(FACC(@/P%(A'(3#55A>C%('# %S3C#"%(/<8('#(7<8%"5'/<8(/8I/<'/;%E(8A5/8I/<'/;%5(/<8(3"#>C%@5(#.(75A<;(A<'%CCA;%<'(/;%<' '%&2<#C#;9(.#"(A<'%;"/C(/557"/<&%(#.('2%(<%'F#"P(5%&7"A'94

O2%(*second task*(#.('2A5(32/5%(#.('2%("%5%/"&2(F/5(8%I#'%8('#('2%(#>$%&'=#"A%<'%8(8%5A;<(#. 1_66(A<('2%(.#"@(#.(5#=&/CC%8(\75%(&/5%(8A/;"/@5\(/A@%8('#(53%&A.9(3/"'A&7C/"(/;%<'n5 .7<&'A#</CA'A%5(/<8(A<'%"/&'A#<5(>%'F%%<(&##3%"/'A<;(/;%<'54(O2%(p75%(&/5%(8A/;"/@5q(53%&A.9 &##"8A</'%8(@7C'AC%I%C(1_66(#3%"/'A#<('2/'(/A@5(/'(3"#&%55A<;(#.('2%('"/..A&(@%55/;%54(*The first level* &#""%53#<85('#('2%(3"#&%55A<;(#.('"/..A&(@%55/;%5(/<8(A5(3%".#"@%8(>9(C#F%"(C%I%C(/;%<'= 8%@#<(:M=%I%<'(Z:M=R[4(*The second level* &#""%53#<85('#('2%(3"#&%55A<;(#.(A<37'('"/..A&(%I%<'5 /<8(A5(3%".#"@%8(>9(?8%<'A.A&/'A#<(/<8(:7'2%<'A&/'A#<(/5(F%CC(/5(:&&%55(1#<'"#C(:M54(H<('2A5(C%I%C 1_66(%S%&7'%5(3"#'%&'AI%(/&'A#<5E(F2A&2(/"%("%/&'A#<(#<('2%(8%'%&'%8(/''%@3'5(#.(A<'"75A#<54(?< 3/"'/CC%CE(/'('2A5(C%I%C('2%(3/''%"<(%S'"/&'A#<(A5(&/""A%8(#7'(>9(/;%<'=8%@#<5(&/CC%8(:M=!(Z\3/''%"<\[4 ?<'%CCA;%<'(A<'"75A#<(8%'%&'A#<(/;%<'5("%/CA]%('2%('2A"8(C%I%C(#.('"/..A&(3"#&%55A<;4(O2%(C/5'(/;%<'5(/"% P<#FC%8;%=>/5%8E(/<8(5#C%I%('2%A"('/5P(A<(&##3%"/'A#<(FA'2(#'2%"(2#5'=>/5%8(/<8(<%'F#"P=>/5%8 /;%<'54(h5%(&/5%(8A/;"/@5E(53%&A.A&/'A#<(#..7<&'A#</CA'A%5(/<8(A<'%"/&'A#<(#.('2%(%<'A"%(5%'(#.('2% /.#"%@%<'A#<%8(/;%<'5(/"%('2%(@/$#"("%57C'5(#.("%5%/"&2(#<('2%(5%&#<8('/5P4

O2%(*Final Report #1*(fYA<J%3)*g(57@@/"A]%8('2%("%57C'5(#.('2%("%5%/"&2(87"A<;('2%('2A"8(/<8 .#7"'2(m7/"'%"5(#.('2%("%5%/"&24(M7"A<;('2A5(3%"A#8('2%(.#CC#FA<;('/5P5(F%"%(5#CI%8B

*[(M%I%C#3@%<'(#.('2%(@#8%C5(#.(8A5'"A>7'%8(&#@@#<(/<8(53%&A.A&(P<#FC%8;%(#.(/;%<'5k

-[(M%I%C#3@%<'(#.('2%(5#.'F/"%(.#"(8A5'"A>7'%8("%3"%5%<'/'A#<(#.(&#@@#<(/<8(53%&A.A& P<#FC%8;%(#.(3/"'A&7C/"(/;%<'5(/<8(A<.#"@/'A#<(5%&7"A'9(595'%@(/5(/(F2#C%k

0[(D#8%CA<;(/<8(3/"'A/C(A@3C%@%<'/'A#<(#.('2%(1/5%(6'789(#.('2%(/;%<'=>/5%8(A<.#"@/'A#< 5%&7"A'9(595'%@4

O2%(@/A<(37"3#5%(#.('2A5(J%3#"'(F/5(\'#(@/P%(5'%3(."#@(@#8%CA<;('#(A@3C%@%<'/'A#<\4(O# @/P%('2A5(\5'%3\(A'(F/5("%U7A"%8('#(&2##5%(2#F(A'(52#7C8(>%(8#<%4(O2%(&2#5%<(5'"/'%;9(#.('2%(1_66 5#.'F/"%(A@3C%@%<'/'A#<(F/5(>/5%8(#<('2%(A8%/(#.('2%(8%I%C#3@%<'(#.(53%&A/CA]%8(*software tool*('2/' &#7C8(3"#IA8%("%75/>ACA'9(#.('2%(@#5'(3/"'(#.('2%(5#.'F/"%(.#"(8%5A;<(/(FA8%("/<;%(#.(/;%<'=>/5%8 <%'F#"P(5%&7"A'9(595'%@54(O2A5(F#"P(A5(I%"9(&#@3C%S(/<8('A@%(&#<57@A<;(/<8(F/5(&/""9A<;(#7' FA'2A<('2A5(/<8(5#@%(#'2%"(3"#$%&'5(87"A<;(C/5'(9%/"4(?'("%57C'%8(A<('2%(8%I%C#3@%<'(#.('2%(5#=&/CC%8 \D7C'A=/;%<'(695'%@(M%I%C#3@%<'(bA'\(ZD:6Mb[4

:&&#"8A<;('#('2%(8%I%C#3%8('%&2<#C#;9(5733#"'%8(>9(D:6Mb('2%(@7C'A=/;%<'(595'%@(@#8%CA<; /<8(A@3C%@%<'/'A#<(#.(/;%<'=>/5%8(1_66(5733#5%('#(5#CI%('F#(2A;2(C%I%C('/5P5B(Z*[(8%I%C#3@%<' #.('2% *System Kernel* #.('2%(1_66E(/<8(Z-[(*Cloning of the software agents*(&#@3"A5A<;(1_66(/<8 8%'/&2@%<'(#.('2%(;%<%"/'%8(@7C'A=/;%<'(595'%@(."#@(695'%@(b%"<%C4

The first task(A<'%<85('#("%3"%5%<'('2%(/33CA&/'A#<(7<8%"(8%I%C#3@%<'(/5(/(@#8%C(A<('%"@5(#.(/ \C/<;7/;%\(53%&A.9A<;(5#=&/CC%8(\695'%@(b%"<%C\4(O#(53%&A.9(695'%@(b%"<%CE('F#(&#@3#<%<'5(#. '2%(8%I%C#3@%<'(5#.'F/"%('##C(/"%(75%84(O2%(.A"5'(#.('2%@(A5(5#=&/CC%8(*Generic Agent* '2/'(/A@5('# 5733#"'(@#8%CA<;(2A;2(C%I%C(53%&A.A&/'A#<(#.(/;%<'(&C/55%5(&/CC%8(/'('2A5(5'/;%(/5(X%<%"A&(/;%<' 57>&C/55%54(?<(./&'E(X%<%"A&(/;%<'(57>&C/55%5(.#"@('2%(5'"7&'7"%(#.('2%(695'%@(b%"<%C4(O2%(5%&#<8 &#@3#<%<'(#.('2%(5#.'F/"%('##C(A5(5#=&/CC%8(*Multi-agent System Development Kit*('2/'(A5(75%8(A<

@#8%CA<;(#.('2%(/33CA&/'A#<=#"A%<'%8(/"&2A'%&'7"%E(8/'/E(P<#FC%8;%E(/<8(&#@@7<A&/'A#< &#@3#<%<'4(O2%(.A"5'('/5P(#.('2%('%&2<#C#;9("%57C'5(A<(MA5'"A>7'%8(b<#FC%8;%(V/5%(J%;A5'%"(/<8 &C/55%5(#.(/;%<'5(&#@3"A5A<;('/"';%'(1_66(Z\X%<%"A&(/;%<'(57>&C/55%5\[4(MA5'"A>7'%8(b<#FC%8;% V/5%(J%;A5'%"(A5(/(@#8%C(#.(8A5'"A>7'%8(P<#FC%8;%(#.('2%(/33CA&/'A#<(7<8%"(8%I%C#3@%<'4(?'(A5(>%A<; 5'#"%8(A<(695'%@(b%"<%C(/<8("%3"%5%<'%8(A<('%"@5(#.(53%&A.A&/'A#<(C/<;7/;%('2/'('2%(695'%@(b%"<%C #3%"/'%5(FA'24(X%<%"A&(/;%<'(57>&C/55%5(/"%(3"#'#'93%5(Z\3/"%<'5\[(#.('2%(5#.'F/"%(/;%<'5(#.(1_66 7<8%"(8%I%C#3@%<'4

O2%(*second task*(/A@5(/'(5#.'F/"%(A@3C%@%<'/'A#<(#.('2%(1_664(?'(5'/"'5(."#@('2%(@#8%C(#.(1_66 "%3"%5%<'%8(A<('%"@5(#.(*System Kernel*(C/<;7/;%(/<8(*Generic agent*(57>&C/55%5(8%I%C#3%8(FA'2A< 3"%IA#75(32/5%4(O2%(.A</C(57>='/5P(#.('2%(5%&#<8('/5P(A5('#(;%<%"/'%('2%(/33CA&/'A#<(A'5%C.4(O2% 8%I%C#3%8('%&2<#C#;9(A5(<#'(I%"9(%/59(A<(75%(F2/'(A5(</'7"/CC9(>%&/75%('2%(1#@37'%"(_%'F#"P 6%&7"A'9(8#@/A<(A'5%C.(A5(I%"9(8A..A&7C'('#(.#"@/CA]%4(D#"%#I%"E(A'(#3%"/'%5(FA'2A<(I%"9 7<3"%8A&'/>C%(/<8(&2/<;%/>C%(%<IA"#<@%<'4(O2%(P%9(&#@3#<%<'(#.(1_66('2/'(A5(P<#FC%8;%(>/5%(#. /<(A<'%CCA;%<'(A<'"75A#<(8%'%&'A#<(595'%@(2/5('#(>%('2%(@/A<(A557%(#.(%/&2('%&2<#C#;9(8%/CA<;(FA'2 '2%(_%'F#"P(6%&7"A'9(8#@/A<4(O2%("%57C'A<;(P<#FC%8;%(>/5%(@75'(>%(\/CAI%\(/<8(3%"@/<%<'C9 /8/3'/>C%('#('2%(%<IA"#<@%<'4(O2%(8%I%C#3%8('%&2<#C#;9(#.(1_66(@#8%CA<;(/<8(A@3C%@%<'/'A#<(A5 .#&75%8(#<(3"#IA8A<;(57&2(/>ACA'A%5(#.(1_664(O275E('2%(*main results*(#.('2A5(32/5%(#.("%5%/"&2(%5(/"% *software tool prototype*(/<8('2%(3/"'A/CC9(A@3C%@%<'%8(@#8%C *of the Case Study* #.(/;%<'=>/5%8 1_664(O2%(3"#;"/@(&#8%(#.('2%(5#.'F/"%('##C(F/5(8%I%C#3%8(%@3C#9A<;(57&2(5#.'F/"% 8%I%C#3@%<'(PA'5(/5(WA57/C(1cc(+4LE(d/I/(-(I%"5A#<(*4O4LE(?VD(eD`(.#"(d/I/(/<8(MVD6(:&&%55= TQ4

O2%(.A</C(32/5%(#.('2%(!"#$%&'("%5%/"&2(52#7C8(>%('2%(8%I%C#3@%<'(/<8(A@3C%@%<'/'A#<(#.('2% 1/5%(6'789E(F2A&2(2/I%('#(A<'%;"/'%('2%(>/5A&('2%#"%'A&/C(/<8(/"&2A'%&'7"/C(A8%/5(8%I%C#3%8(/' 3"%IA#75(32/5%5(#.('2%("%5%/"&24(O2%(>%C#F(@/'%"A/C5(#7'CA<%5('2%(8%I%C#3%8(1/5%(6'7894

1.3. High-level Architecture of the Case Study

O2%(/;%<'=>/5%8(/"&2A'%&'7"%(#.('2%(&#@37'%"(<%'F#"P(5%&7"A'9(595'%@(F/5(3"#3#5%8(A< fX#"#8%'5PA*(*et al*=LLg(/<8(fX#"#8%'5PA-(*et al*=LLg4(O2%(8%I%C#3%8(&/5%(5'789(A5(/<(A@3C%@%<'/'A#< #.(/(3/"'A&7C/"(5A@3CA.A%8(&/5%(#.('2A5(/"&2A'%&'7"%4

V%C#F(A<('2%(&/5%(5'789(F%(&#@37'%"(<%'F#"P(&#<5A5'A<;(#.(.#7"(2#5'5(ZYA;4*4*[4 O2A5(<%'F#"P(&/<(&#@3"A5%(5%I%"/C(5%;@%<'5(#.(/(`:_(/<8('2%(A<37'('"/..A&(&/<(>%(>#'2(A<5A8%(/<8 #7'5A8%(`:_('"/..A&4(R/&2(2#5'(A5(3"#'%&'%8(>9(/<(A<'%;"/'%8(/;%<'=>/5%8(5%&7"A'9(595'%@ &#@3"A5A<;(5%I%"/C(53%&A/CA]%8(*agent-demons*(Z:M[(@#<A'#"A<;('2%(A<37'('"/..A&(/<8(%S'"/&'A<; 3"%8%.A<%8(5A;<A.A&/<'(%I%<'5(/<8(3/''%"<5(."#@('2%(5%U7%<&%(#.(*IP*=3/&P%'5E(*access control*(/;%<'E *authentication and identification*(/;%<'(/<8(P<#FC%8;%=>/5%8(*intrusion detection*(/;%<'54(O2%5% /;%<'5(A<'%"/&'(87"A<;('2%A"(#3%"/'A#<(IA/(@%55/;%5(%S&2/<;%('275(5733#"'A<;(&##3%"/'AI%(@7C'A= C%I%C(A<37'(8/'/(3"#&%55A<;4

R/&2(@%55/;%(#.(/<(/;%<'(A5("%3"%5%<'%8(A<(bmD`(C/<;7/;%4(O2%(@%55/;%(3"#IA8%5 A<5'"7&'A#<5(.#"('2%(/;%<'="%&%AI%"(2#F('#(3"#&%55('2%(@%55/;%(/<8(2#F('#("%/&'('#(A'E(/<8(53%&A.A%5 '2%(&#<'%<'(#.('2%(@%55/;%4(O2%(@%55/;%(&#<'%<'(A5("%3"%5%<'%8(A<('%"@5(#.(eD`(C/<;7/;%(/<8 53%&A.A%5(/<(#>$%&'(FA'2(/55A;<%8(/''"A>7'%(I/C7%54(O2%(#>$%&'(A5(7<8%"5'##8(/5(/(5A;<A.A&/<'(%I%<'(#" /(3/''%"<(FA'2(/55A;<%8(/''"A>7'%5E(./&'5(/>#7'(8%'%&'%8(/''%@3'5('#(>"%/P(A<('2%(/&&%55%5(&#<'"#C 595'%@(#"(/7'2%<'A&/'A#<(/<8(A8%<'A.A&/'A#<(595'%@E(/<8(/>#7'(#'2%"(5753A&A#75(/&'AIA'A%5(#"(/''%@3'5 #.(/''/&P5(8%'%"@A<%8(>9(/<(/;%<'=8%@#<4

R/&2(/;%<'(3"#&%55%5('2%(8%'%"@A<%8(5A'7/'A#<(/&&#"8A<;('#(/(3"%8%.A<%8(5&%</"A#(/<8(5%<85(/ @%55/;%('#(/<(A<'"75A#<(8%'%&'A#<(/;%<'(/<8a#"(#'2%"(/;%<'=8%@#<4(O2%(@%55/;%5(3"#&%%8A<;(."#@ /<(A<'"75A#<(8%'%&'A#<(/;%<'(&/<(>%('F#.#C84(O2%(.A"5'('93%(#.(@%55/;%5(A5(/88"%55%8('#(/<(/;%<' A<5A8%('2%(2#5'(A<5'"7&'A<;(A'('#(>"%/P(/(&#<<%&'A#<(#"('#(.#&75(/''%<'A#<(#<(/(&#""%<'(&#<<%&'A#<(A.(/ 5753A&A#75(/&'AIA'9(2/5(>%%<(8%'%"@A<%84(O2%(5%&#<8('93%(#.(@%55/;%5(A5(/88"%55%8('#('2%(A<'"75A#< 8%'%&'A#<(/;%<'(#.(#'2%"(2#5'4(?<('2A5(&/5%('2%(@%55/;%(&#<'%<'(Z\#>$%&'\[(A5('2%(A<.#"@/'A#<(/>#7' 8%'%&'%8(5753A&A#75(75%"i5(>%2/IA#"(#"(/>#7'('2%(A<'"75A#<4(:<(%S/@3C%(#.(bmD`(@%55/;%(5%<'(>9 \?<37'(O"/..A&(D#8%C\(&#@3#<%<'('#('2%(/;%<'(:M=R(A5(/5(.#CC#F5B

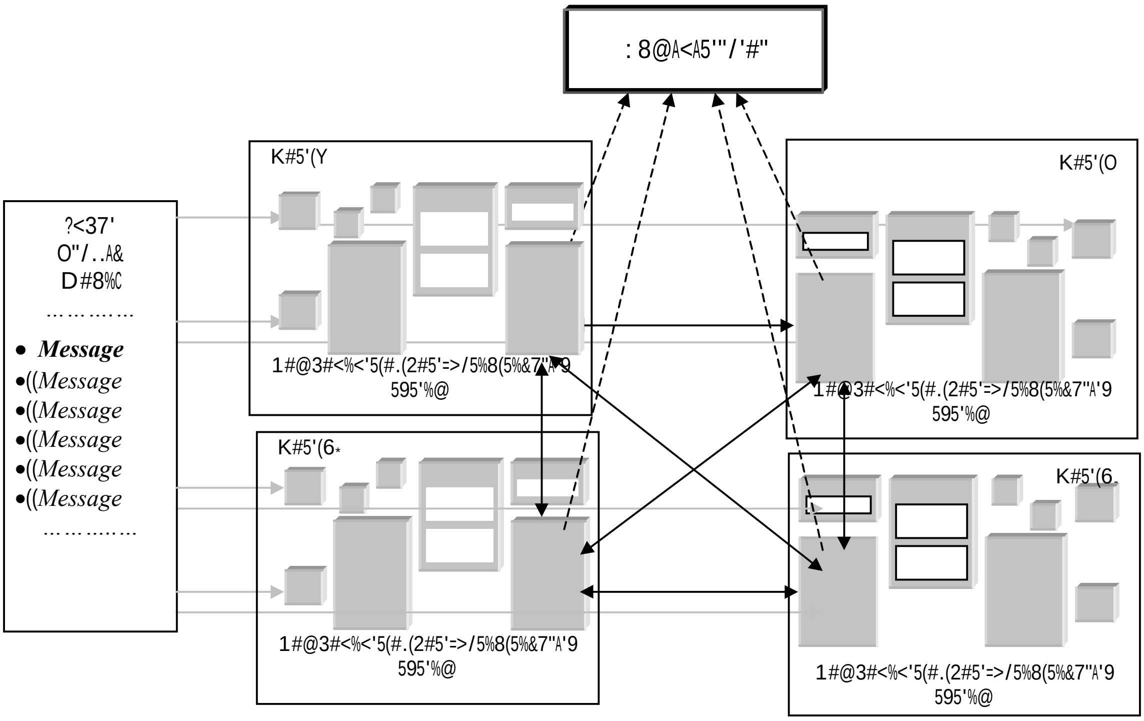


Fig.1.14(h33%"(C%I%C(/"&2A'%&'7"%(#.('2%(&/5%(5'789

```
Performative: tell
    Sender: Input Traffic Model
    Receiver: AD-E (host S1)
    Content: <content>
    Ontology: ISS
    Language: XML
```

O2%(&#<'%<'(#.('2A5(@%55/;%(A<(e D `(C/<;7/;%(A5(3"%5%<'%8(A<('2%(733%"=C%.'(&#"<%"(FA<8#F A<(YA;4*4*-4

O2%"%(A5(<#(3/"'A&7C/"(733%"=C%I%C(@/</;A<;(5#.'F/"%('2/'(&##"8A</'%5(2#5'=>/5%8(/;%<' #3%"/'A#<(/5(F%CC(/5(A<'"75A#<(8%'%&'A#<(/;%<'5(#.(8A..%"%<'(2#5'5(#.('2%(&#@37'%"(<%'F#"P4(O2% @7C'A=/;%<'(5%&7"A'9(595'%@(#3%"/'%5(A<('2%(8A5'"A>7'%8(F/94

O2%(\?<37'(O"/..A&(@#8%C\(5#.'F/"%(Z5%%(YA;4*4*[(5A@7C/'%5('2%(A<37'('"/..A&4(O2%(#7'37'(#. '2A5(3"#;"/@(A5(/("/<8#@(5%U7%<&%(#.(*IP*-3/&P%'5('2/'(A5(/(@AS'7"%(#.(<#"@/C(/<8(/><#"@/C(5'"%/@5 #.(%I%<'54

O2%(/><#"@/C(5'"%/@(#.(%I%<'5(A5(5A@7C/'A<;(/''/&P5(/;/A<5'('2%(&#@37'%"(<%'F#"P4(Y#"(%I%"9 2#5'('2%(5#.'F/"%(&#@3#<%<'(\?<37'(O"/..A&(D#8%C\(A5(;%<%"/'A<;('2%(A<37'('"/..A&(A<('2%(.#"@(#. 5%U7%<&%(#.(#7'37'5(#.('2%(*tcpdump*(3"#;"/@4(Y#"(%S/@3C%E(5A@7C/'%8(*SYN-port scanning*(A<37' 5%U7%<&%(&#7C8(>%(/5(.#CC#F5B

```
*BLLBLL4L,OLO,((*,Q4*L-4*4*4*LNQ((r((*T*4*+Q4*4-4-*B((6((*-NGG*GB*-NGG*GZL[
*BLLBLL4GOO-O,((*,Q4*L-4*4*4*LNQ((r((*T*4*+Q4*4-4-OB((6((*-NGG*GB*-NGG*GZL[
*BLLBLL4T-O,G+((*,Q4*L-4*4*4*LNQ((r((*T*4*+Q4*4-4-NB((6((*-NGG*GB*-NGG*GZL[
   s s s s s s s s s s s s s s s s s s s s s s s s s s s s
*BLLB*L4LGQTLO((*,Q4*L-4*4*4*LNQ((r((*T*4*+Q4*4-4-LGTB((6((*-NGG*GB*G,GG*GZL[(((4
```

: <(/''/&P(/'('2%(/33CA&/'A#<(C%I%CE(/("%@#'%(/''/&P(%S%&7'A<;(&#@@/<85(#.('2%(#3%"/'A#< 595'%@(#"(%S%&7'A<;(/33CA&/'A#<(595'%@(&/CC5(/"%(53%&A.A%8(A<('%"@5(#.(/(5%U7%<&%(#.('2%(*tcpdump* @%55/;%5(%S3/<8%8(>9('2%(*Data Field*\(F2A&2(53%&A.A%5('2%(@%55/;%(5%@/<'A&54

O2%(#7'&#@%(#.(%/&2(/''/&P(&/<('/P%(*successful*\(#"(*unsuccessful*\(I/C7%4(O2A5(#7'&#@%(A5 5A@7C/'%8(#<('2%(>/5A5(#.(/("/<8#@A]/'A#<(3"#&%87"%4(?<37'(""/..A&(@#8%C(75%5(8/'/(/>#7'(*IP*= /88"%55%5(#.('2%(/''/&P%8(&#@37'%"(<%'F#"P(2#5'5(/<8(A<.#"@/'A#<(/>#7'('2A5(<%'F#"P &#<.A;7"/'A#<4(R/&2(/''/&P(&/<(>%(5A@7C/'%8(/&&#"8A<;('#('2%(3/"'A&7C/"(5&%</"A#(Z5%%(5%&'A#<(*4+ >%C#F[(/<8('#('2%(3/"'A&7C/"(3%"&%<'/;%(#.(<#"@/C(/<8(/><#"@/C(""/..A&4

H'2%"(&#@3#<%<'5(#.('2%(&/5%(5'789(/"%(\J%/C(OA@%(D#8%C\(/<8(75%"(A<'%"./&%('2/'(@/P%5 3#55A>C%('#(IA57/CA]%(3%".#"@/<&%(#.('2%(3/"'A&7C/"(&#@3#<%<'5(#.('2%(@7C'A=/;%<'(5%&7"A'9(595'%@4

O2%(5#.'F/"%(&#8%(A5(F"A''%<(#<('2%(>/5A5(#.(WA57/C(1ccE(d:W:(-(/<8(eD`(5#.'F/"% 8%I%C#3@%<'(PA'54

1.4. More Detailed Architecture of Host-based Security Components

`%'(75(&#<5A8%"(/"&2A'%&'7"%(#.('2%(2#5'=>/5%8(3/"'(#.('2%(@7C'A=/;%<'(1_66(ZYA;4*4-[4(O2% >/5A&(2#5'=>/5%8(&#@3#<%<'5(/"%(/;%<'=8%@#<5(8%<#'%8(>9(tM=RE(:M=!*E(:M=!-E(:?: Z/7'2%<'A&/'A#<(/<8(A8%<'A.A&/'A#<(/;%<'[(/<8(:1:(Z/&&%55(&#<'"#C(/;%<'[(/<8('F#(P<#FC%8;%=>/5%8 /;%<'5(=(?M:*(/<8(?M:-(Z?<'"75A#<(M%'%&'A#<(:;%<'5[4

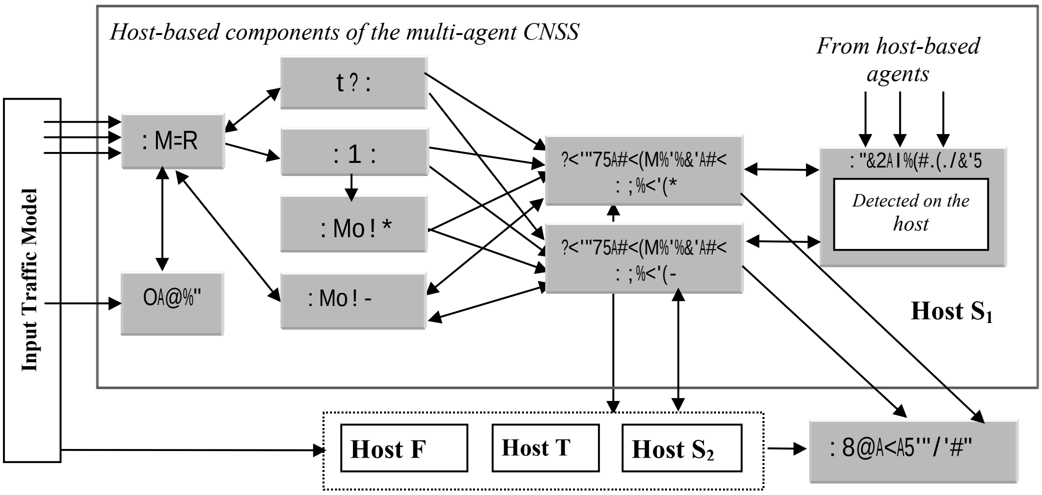


Fig.1.2.(:"&2A'%&'7"%(/<8(A<'%"/&'A#<(#.(2#5'=>/5%8(3/"'(#.('2%(@7C'A=/;%<'(1_66

Agent-demon AD-E(A5("%53#<5A>C%(.#"('2%(A<37'(""/..A&(3"%3"#&%55A<;4(?'(@#<A'#"5(""/..A& /A@A<;(/'(%S"'/&'A#<(#.(5%U7%<&%5(#.(5#=&/CC%8(\%I%<'5\('2/'(/"%(5%@/<'A&/CC9(@%/<A<;.7C(/<8 /55#&A/'%8(FA'2('2%(&7""%<'(&#<<%&'A#<54(O2%5%(%I%<'5(/"%(5#""'%8E(5'#"%8(A<(*AD-E*(8/'/>/5%(/<8(%/&2 #.(57&2(%I%<'5(A5(5%<'(.#"('2%(3#5'%"A#"(3"#&%55A<;('#(#<%(#"(5%I%"/C(/;%<'=8%@#<5(Z5%%(YA;4*4-[4

*Agent-*8%@#<5(.#"(A8%<'A.A&/'A#<(/<8(/7'2%<'A&/'A#<(Z:?:[(/<8(/&&%55(&#<'"#C(Z:1:[(3%".#"@ '2%A"(&#<I%<'A#</C(.7<&'A#</CA'A%5E("%&#"8('2%("%57C'5(A<'#('2%A"(8/'/(>/5%5(/<8(5%<8(@%55/;%5('#('2% *Intrusion detection agent*(A./(5753A&A#75(>%2/IA#"(#"(/''%@3'(#.(/<(/''/&P(2/5(>%%<(8%'%&'%84(:?: /;%<'(A5("%53#<5A>C%(.#"(A8%<'A.A&/'A#<(#.('2%(@%55/;%5(5#7"&%(/88"%55(/<8(.#"(&#<.A"@/'A#<(#.('2%A" /7'2%<'A&A'94(:1:(/;%<'(@/</;%5(75%"5i(/&&%55(A<(&#<.#"@A'9(FA'2('2%A"(/&&%55("A;2'5(/<8(C/>%C5(#. &#<.A8%<'A/CA'9(#.('2%(3"#'%&'%8(#>$%&'54(O2%5%(/;%<'5(8%'%&'(/''%@3'5(#.('2%(7</7'2#"A]%8(/&&%55('# '2%(2#5'(A<.#"@/'A#<("%5#7"&%5E(8%'%&'5(A<'%""73'(%I%<'5(*Authentication failure" /*<8 *"Unauthorized access"*E(""/3('2%5%(%I%<'5(/<8(A<.#"@(/>#7'(57&2(%I%<'5('2%(?M:-4

Agent-demons(*AD-P1* /<8 *AD-P2*(/"%("%53#<5A>C%(.#"(%S"'/&'A#<(#.('2%(3"%8%.A<%8 Z\A<'%"%5'A<;\E(\@%/<A<;.7C\[(3/''%"<5(#.(\%I%<'5\(/<8(@/PA<;(8%&A5A#<5(Z>#'2(3"%CA@A</"9(/<8 .A</C[(/>#7'(/''%@3'5(#.(/''/&P5(#"(5753A&A#75(>%2/IA#"(#.(75%"5(&#<<%&'%8(FA'2('2%(2#5'4(?<('2% A@3C%@%<'%8(&/5%(5'789('2%(/;%<'(:M=!*(A5("%53#<5A>C%(.#"(%S"'/&'A<;(3/''%"<5('2/'(&#""%53#<85('#

'2%(5753A&A#75(>%2/ IA#"(#"(/''%@3'5(#.(/''/&P5(CAP%(*port scanning*(Z#<(/33CA&/'A#<(C%I%C[E(*finger search*(/<8(*buffer overflow*4(O2%(/;%<'(: M=! -(A5(A<'%<8%8('#(%S'"/&'(3/''%"<5(&#""%53#<8A<;('#('2% *denial of service*(/''/&PE(*syn-flood*(/''/&P(/<8(*port scanning*(Z#<(<%'F#"P(/<8('"/<53#"'(C%I%C[4

O2%(5753A&A#75(%I%<'5(/<8(3/''%"<5(8%'%&'%8(>9(/;%<'=8%@#<5(/"%(5%<'('#(?M : *(/<8a#"(?M : - /<8(5#@%(#.('2%@(/"%("%&#"8%8(A<'#('2%(p : "&2AI%(#.(./&'5q4(?M : *(/<8(?M : -(75%('2%5%(./&'5('# 3%".#"@(P<#FC%8;%=>/5%8(3"#&%55A<;(#.('2%(A<.#"@/'A#<("%&%AI%8(."#@(/;%<'=8%@#<54

Database "Archive of facts"(5'#"%5(8/'/(/>#7'(3/5'(Z2/I%(>%%<(#I%"[(&#<<%&'A#<54(O2%5%(8/'/ /"%(75%8(>9(?M : *(/<8(?M : -(.#"(8%'%&'A#<(8A5'"A>7'%8(@7C'A=32/5%(/''/&P5(F2%<(A'(A5(<%&%55/"9('# 3"#&%55(&7""%<'(/<8(3/5'(&#<<%&'A#<5('#("%&#I%"('2%(5&%</"A#(#.(/''/&P(/<8(@/'&2('#(/(P<#F< 5&%</"A#4(_#'A&%('2/'(8%'%&'A#<(#.(/(5&%</"A#(#.('2%(/''/&P(A5(3#55A>C%(#<C9(/5(/("%57C'(#.(&##3%"/'A#< #.(5%I%"/C(/;%<'54

Intrusion detection agents(Z?M : [(/"%("%53#<5A>C%(.#"(2A;2=C%I%C(A<37'(8/'/(3"#&%55A<;E(/<8 @/P%("7C%=>/5%8(8%&A5A#<5(#<('2%(>/5A5(#.(A<37'(./&'5(&#<'/A<%8(A<("%&%AI%8(@%55/;%54(O2%9(&/< "%&%AI%(@%55/;%5(/>#7'(8%'%&'%8(5753A&A#75(>%2/IA#"(/<8(/''%@3'5(#.('2%(/''/&P(."#@(/;%<'=8%@#<5 #.('2%(5/@%(2#5'(/5(F%CC(/5(@%55/;%5(."#@(5%&7"A'9(/;%<'5(#.('2%(#'2%"(2#5'54(O2%(8A5'A<&'A#< >%'F%%<(?M : *(/<8(?M : -(A5('2/'('2%9(3"#&%55(8A..%"%<'(5A'7/'A#<54(?M : *(3"#&%55%5(5A'7/'A#<5(/"A5A<; 87%('#(&#@>A<%8(53##.A<;(/''/&P5(F2%"%/5(?M : -(3%".#"@5(2A;2(C%I%C(3"#&%55A<;(#.(./&'5(/A@A<;(/' 8%'%&'A#<(#.(8A5'"A>7'%8(@7C'A=32/5%(/''/&P54(?M : -(A5(A<'%<8%8('#(8%'%&'(57&2(/''/&P5(#"(&#@3#<%<'5 #.(/''/&P5(/5

Z*[(*Reconnaissance*E('2/'(&#""%53#<85('#('2%(&#CC%&'A<;((;%<%"/C(8/'/(/>#7'(&#@37'%"(<%'F#"P &#<.A;7"/'A#<E(A8%<'A.A&/'A#<(#.('2%(2#5'5(&#@3"A5A<;(<%'F#"PE(/&&%55A>C%(5%"IA&%5E A8%<'A.A&/'A#<(#.('2%(#3%"/'A#<(595'%@E(/33CA&/'A#<5(%'&4

Z-[(*Host penetration*('2/'(A5(/(@/C%./&'#"(/&'AIA'9(/A@%8(/'(3%<%'"/'A#<(A<'#(&#@37'%"(<%'F#"P4

ZO[(*Privileges escalating*('2/'(A5(/(@/C%./&'#"i5(/''%@3'('#(;%'(%S3/<8%8(/&&%55("A;2'54

ZG[(*Deepening penetration*(#<(2#5'('2/'(A5(%S3/<8A<;(@/C%./&'#"i5(/&&%55('#(.AC%5E(.#C8%"5(/<8 3"#;"/@5(#.('2%(2#5'

ZN[(*Deepening penetration through net*('2/'(A5(%S3/<8A<;(@/C%./&'#"i5(/&&%55('#(.AC%5E(.#C8%"5(/<8 3"#;"/@5(#.('2%(#'2%"(2#5'5(#.('2%(&#@37'%"(<%'F#"P(7<8%"(/''/&P4

V#'2(?M : *(/<8(?M : -(2/I%(5A@AC/"(/"&2A'%&'7"%(/<8('2%(#<C9(8A5'A<&'A#<(A5('2%(&#<'%<'(#.('2%A" P<#FC%8;%(>/5%5(ZbV[(&#@3"A5A<;('2%("7C%5E(75%8('#(@/P%(8%&A5A#<5(#<('2%(>/5A5(#<(A<37'(./&'54

_#'A&%('2/'(%/&2(/;%<'(#.('2%(2#5'(2/I%(/(C#&/C(8/'/>/5%(F2A&2(A5(/&&%55A>C%(.#"(%I%"9(2#5'= >/5%8(/;%<'4(?<(./&'E(/C'#;%'2%"('2%9(.#"@(8A5'"A>7'%8(8/'/>/5%(#.('2%(2#5'=>/5%8(5%&7"A'9(595'%@4

O2%(.7<&'A#</CA'9(#.('2%(5#.'F/"%(&#@3#<%<'(\ : 8@A<A5'"/'#"\(A5('#(3"#IA8%(/(75%"(>9 4.0M

1.5. Agent Architecture

:CC(2#5'=>/5%8(5%&7"A'9(/;%<'5(/"%(A@3C%@%<'%8(#<('2%(>/5A5(#.(/(5'/<8/"8(/"&2A'%&'7"% 8%3A&'%8(A<(YA;4*4O4(O2%(8A5'A<&'A#<5(/"%(#<C9(A<(P<#FC%8;%(>/5%5(&#<'%<'54(O2%(/;%<'(8%@#<5i(bV &#<'/A<(#<C9(5A@3C%("7C%5(.#"(%S'"/&'A<;(%I%<'5(#"(3/''%"<5(F2%"%/5(A<'"75A#<(8%'%&'A#<(/;%<'5(2/I% @#"%(&#@3"%2%<5AI%(bV54(`%'(75(#7'CA<%('2%(;%<%"A&(/"&2A'%&'7"%(#.(/;%<'54

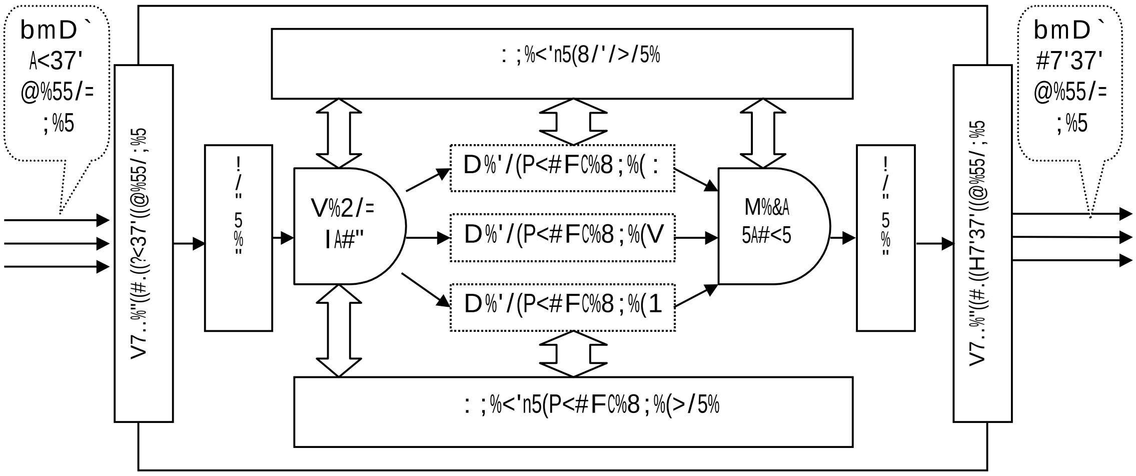


Fig.1.3.(6%&7"A'9(/;%<'(/"&2A'%&'7"%

Buffer of input messages(A5(75%8(.#"(A<37'(@%55/;%5(5'#"A<;E(#"8%"A<;(/<8(59<&2"#<A]/'A#<(#. '2%A"(3"#&%55A<;4(`%'(75("%@A<8('2/'(/CC(@%55/;%5(/"%("%3"%5%<'%8(A<(bmD`(.#"@/'E(F2#5%(&#<'%<' A5(53%&A.A%8(A<('%"@5(#.(eD`(C/<;7/;%4

Parser(3%".#"@5(59<'/&'A&/C(/</C95A5(/<8(A<'%"3"%'/'A#<(#.(@%55/;%54(O2%(5A@AC/"(3"#;"/@ 3%".#"@5(;%<%"/'A#<(/<8(5%<8A<;(#.(#7'37'(@%55/;%54(O#(A<'%"3"%'('2%(A<37'(/<8('#(;%<%"/'%('2% #7'37'(@%55/;%(! /"5%"(2/5('#(/&&%55('#('2%(8#@/A<(#<'#C#;9(#.('2%(/;%<'E(F2A&2(A5(/(3/"'(#.('2% *Agent's database*4

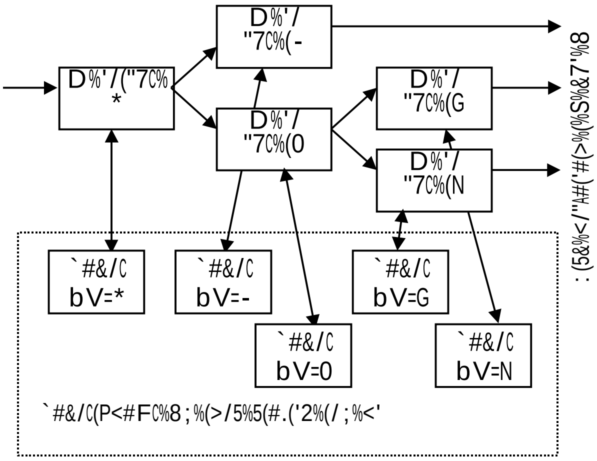


Fig.1.4.(:<(%S/@3C%(#.('2%(/;%<'i5 P<#FC%8;%(>/5%(/"&2A'%&'7"%

O2%(A<'%"3"%'%8(@%55/;%(&#<'%<'(A5('2%(A<37'(#.('2%(&#@3#<%<'(*Behavior*E(F2A&2(2/5('# 8%'%"@A<%('2%(F/9(#.(A<37'(@%55/;%(3"#&%55A<;4(?'(;%<%"/'%5(/(5&%</"A#(#<('2%(>/5A5(#.('"%% 5'"7&'7"%8(*Meta-knowledge base*E(F2A&2(A.(<%&%55/"9(8%"AI%5(/(8%&A5A#<(IA/(/&&%55A<;(*Local* *knowledge bases*(/55#&A/'%8(FA'2('2%(<#8%5(#.('2%(@%'/=P<#FC%8;%(>/5%(5'"7&'7"%4(?.(<%&%55/"9('2% 8%&A5A#<=@/PA<;(3"#&%87"%(75%5(8/'/(/>#7'(3"%=2A5'#"9(#.('2%(/;%<'(>%2/IA#"4(O2A5(8/'/(/"% &#<'/A<%8(A<('2%(*Agent's database.*(O2%(5%U7%<&%(#.(5'%35(#.('2%(5&%</"A#('#(>%(%S%&7'%8(A5 8%'%"@A<%8(>9('2%(<#8%5('2/'(CA%(/C#<;('2%("%/CA]%8(F/9(."#@('2%("##'('#('2%(C%/.(#.('2%(@%'/= P<#FC%8;%(>/5%(5'"7&'7"%4(:<(%S/@3C%(#.('2%(@%'/=P<#FC%8;%(>/5%(5'"7&'7"%(/<8(A'5(CA<P5('#(C#&/C P<#FC%8;%(>/5%(A5(;AI%<(A<(YA;4*4G4

:("%53#<5A>ACA'9(#.('2%(*Decision*(&#@3#<%<'(A5('#(8%'%"@A<%(/("%/&'A#<(#.('2%(/;%<'(A<('2% "%57C'(#.('2%(5&%</"A#(%S%&7'A#<4(O2%"%(/"%('F#(3#55A>C%("%/&'A#<5B(Z*[(;%<%"/'A#<(#.(/<(#7'37' @%55/;%Z5[(/<8(Z-[("%&#"8A<;('2%("%57C'(#.('2%(5&%</"A#(%S%&7'A#<(A<('2%(/;%<'i5(8/'/>/5%4(O2%(C/''%" /5(/("7C%(&#""%53#<85('#(/<(A<'%"@%8A/'%(8%&A5A#<(@/8%(>9('2%(/;%<'('2/'(A5(5733#5%8('#(>%(75%8 C/'%"4

1.6. Input Traffic Model: Scenarios of Combined Distributed Attack

O2%(@#8%C(#.(A<37'('"/..A&(&#""%53#<85('#(/(<7@>%"(#.(5&%</"A#5('2/'(/"%(75%8(>9(/ @/C%./&'#"4(:(5&%</"A#(&/<(&#<5A5'(#.(/(57>5%'(#.(/''/&P5('2/'(/"%

*4(6&/<<A<;(#.(/(2#5'(3#"'5(/A@A<;(/'(8%'%"@A</'A#<(#.('2%(/&'AI%(3#"'5(/<8(/I/AC/>C%(5%"IA&%5(Z.'3E '%C<%'E(%'&4[4

-4(:''%@3'5(#.(&#<<%&'A#<('#(/(2#5'(#<(/(5%"IA&%(CAP%(.'3E('%C<%'E(%'&4(75A<;(8A..%"%<'(5#7"&%(?!= /88"%55%5(/<8(;7%55A<;(3/55F#"84

O4(1#@>A<%8(53##.A<;(/''/&P4(O2A5(/''/&P(/;/A<5'(/(&#@37'%"(<%'F#"P(&#@3"A5%5(5%I%"/C(5'%354 YA"5'E('2%(@/C%./&'#"(%5'/>CA52%5(/(*IP*=&#<<%&'A#<(#<(/(2#5'(6(/<8(;%'5(/<(A<A'A/C(<7@>%"(#.('2% &#<<%&'A#<4(_%S'E(2%("%/CA]%5(*denial of service*(/''/&P(/;/A<5'(/('"75'%8(2#5'(O(/<8(87"A<;(O 2/<;=73(2%(%5'/>CA52%5(/(*IP*=&#<<%&'A#<(#<('2%(2#5'(6(#<(>%2/C.(#.('2%('"75'%8(2#5'(O4(O2%(2#5' 6(5%<85('#('2%(2#5'(O('2%(&#<.A"@/'A#<("%&%A3'4(O2%(&#<&C78A<;(#3%"/'A#<(#.('2%(@/C%./&'#"(A5 5%<8A<;("%3C9("%&%A3'('#('2%(2#5'(6(."#@(A'5(2#5'(e(A<5'%/8(#.('2%(2#5'(O('275(/55A;<A<;('#('2% 2#5'(e(%S'%<8%8(/&&%55("A;2'5(F2A&2('2%('"75'%8(2#5'(O(3#55%55%54

G4(:''%@3'5('#(;%'(7</7'2#"A]%8(/&&%55('#(.AC%5(#.(/(2#5'4

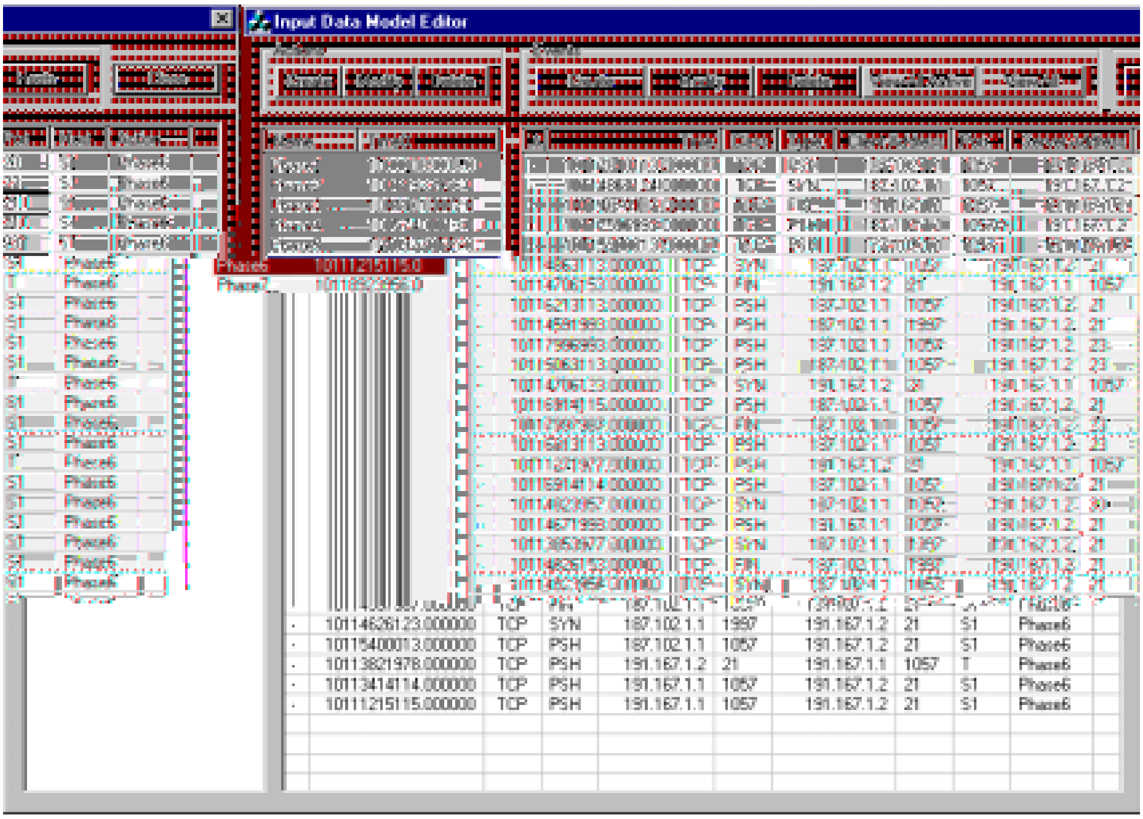
N4(V7..%"(#I%".C#F(/''/&P(#<(/(2#5'(/A@A<;(/'(>##5'A<;(#.('2%(/&&%55("A;2'54

O2%(A<37'('"/..A&(@#8%C(&/<("%/CA]%(/("%/5#</>C%(5%U7%<&%(#.('2%5%(\5A<;C%=32/5%\(/''/&P5 75A<;(8A..%"%<'(%<'"9(3#A<'5(Z2#5'5[4(O2%5%(/''/&P5(.#"@('2%(733%"=C%I%C(53%&A.A&/'A#<(#.(/(8A5'"A>7'%8 @7C'A=32/5%(/''/&P4(?<('7"<E(%/&2(/''/&P(Z%/&2(32/5%(#.(/(8A5'"A>7'%8(/''/&P[(A5(5A@7C/'%8(>9(/ 5%U7%<&%(#.(*IP*=3/&P%'5(#.(A<37'('"/..A&E(F2A&2(A5(/(@AS'7"%(#.(<#"@/C(/<8(/><#"@/C(75%"5i(/&'AIA'94 O2%5%(5%U7%<&%5(.#"@('2%(C#F=C%I%C(@#8%C(#.('2%(%I%"9(32/5%(#.(/<(/''/&P4(V%C#F(/(3/"'A&7C/" 5&%</"A#(#.(/(8A5'"A>7'%8(/''/&P(8%@#<5'"/'%5('2%(#3%"/'A#<(#.('2%(&/5%(5'7894

?<(./&'E(\?<37'(O"/..A&(D#8%C\(A5(/(8/'/>/5%E(F2A&2(A5(5'#"A<;('2%(5%U7%<&%(#.(*IP*=3/&P%'5('2/' A5(5733#5%8('#(>%(75%8(/5('2%(A<37'(#.(/(2#5'4(:(3/"'A&7C/"(3"#;"/@('2/'(A5(8%I%C#3%8(/<8 A@3C%@%<'%8(/5(/(5#.'F/"%('##C(5A@7C/'A<;(<#"@/C(/><#"@/C(A<37'('"/..A&(;%<%"/'%5('2%(&#<'%<' #.('2A5(8/'/>/5%4(h33%"=C%I%C(75%"(A<'%"./&%(#.('2A5('##C(A5(8%3A&'%8(A<(YA;4*4N4

`%.'=2/<8(/"%/(#.('2%(A<'%"./&%(FA<8#F(A5(75%8('#(C#/8E(%8A'(/<8(8%3A&'('2%(</@%5(#.(5A<;C%= 32/5%(/''/&P5('2/'(&#""%53#<8('#(/(5A@7C/'%8(@7C'A=32/5%(/''/&P4(O2%(5%U7%<&%(#.('2%5%(</@%5(A< '2A5(FA<8#F(&#""%53#<85('#('2%(#"8%"(#.('2%A"("%/CA]/'A#<(/5('2%(@7C'A=32/5%(/''/&P4(?<('2%("A;2'=2/<8 FA<8#F('2%(5%U7%<&%(#.('2%(*IP*=3/&P%'5(&#@3#5A<;('2%(@/"P%8(5A<;C%=32/5%(/''/&P(Z@/"P%8(A<('2% C%.'=2/<8(FA<8#F[(A5(8%3A&'%84(O2%(5/@3C%5(#.(5A<;C%(32/5%(/''/&P5(&/<(>%(C#/8%8(@/<7/CC9('2"#7;2 75%"(A<'%"./&%(#"(&/<(>%(&#3A%8(."#@(/('"/..A&(.AC%(Z/78A'(8/'/(.AC%[(&#<'/A<A<;(/(."/;@%<'(#.(/78A' 8/'/(&#""%53#<8A<;('#('2%(/''/&P(#.('2%("%53%&'AI%('93%4(_#'A&%('2/'(5%U7%<&%5(#.(?!=3/&P%'5 &#""%53#<8A<;('#(8A..%"%<'(&#<<%&'A#<5(&/<(>%(@AS%8(A<(/<(/">A'"/"9(F/94

`%'(75(%S3C/A<(A<(>"A%.(2#F(/(@#8%C(#.(/(&#@>A<%8(/''/&P(A5(&#@3#5%84(O2%(.A"5'(5'%3(A5('# 8%.A<%('2%(5%U7%<&%(#.(32/5%5(#.('2%(&#<5'"7&'%8(/''/&PE(A4%4('2%(5%U7%<&%(#.(</@%5(#.(\5A<;C% 32/5%\(/''/&P54(O2A5(5%U7%<&%(8%'%"@A<%5('2%(2A;2(C%I%C(53%&A.A&/'A#<(#.('2%(/''/&P('#(>%(5A@7C/'%84 O2%(<%S'(5'%3(#.(/''/&P(&#@3#5A'A#<(A5('#(@/3(/(5%U7%<&%(#.(*IP*=@%55/;%5('#(%/&2(</@%(#.(\5A<;C%= 32/5%(/''/&P\(8%'%"@A<%8(A<('2%(/.#"%@%<'A#<%8(5&%</"A#4(*IP*=@%55/;%5(2/I%('#(>%(%8A'%8('#(/55A;< '2%('A@%(#.(%/&2(\5A<;C%=32/5%\(/''/&P(>%;A<E(/<8(#'2%"(/''"A>7'%54(O2%(5%&#<8(5'%3(#.(%8A'A#<(A5('#



·	10114863113.000000	TCP	SYN	187.102.1.1	1057	191.167.1.2	21		
·	10114706153.000000	TCP	FIN	191.167.1.2	21	191.167.1.1	1057		
·	10116213113.000000	TCP	PSH	187.102.1.1	1057	191.167.1.2	21		
·	10114591993.000000	TCP	PSH	187.102.1.1	1997	191.167.1.2	21		
·	10117996993.000000	TCP	PSH	187.102.1.1	1057	191.167.1.2	23		
·	10115063113.000000	TCP	PSH	187.102.1.1	1057	191.167.1.2	23		
·	10114706123.000000	TCP	SYN	191.167.1.2	21	191.167.1.1	1057		
·	10116914115.000000	TCP	PSH	187.102.1.1	1057	191.167.1.2	21		
·	[illegible]	TCP	FIN	[illegible]	1057	191.167.1.2	23		
·	10115813113.000000	TCP	PSH	187.102.1.1	1057	191.167.1.2	23		
·	10111221977.000000	TCP	PSH	191.167.1.2	21	191.167.1.1	1057		
·	10116914114.000000	TCP	PSH	187.102.1.1	1057	191.167.1.2	21		
·	10114023957.000000	TCP	SYN	187.102.1.1	1057	191.167.1.2	20		
·	10114671993.000000	TCP	PSH	191.167.1.1	1057	191.167.1.2	21		
·	10113953977.000000	TCP	SYN	187.102.1.1	1997	191.167.1.2	21		
·	10114826153.000000	TCP	FIN	187.102.1.1	1997	191.167.1.2	21		
·	[illegible]	TCP	SYN	[illegible]	1057	191.167.1.2	21		
·	10114626123.000000	TCP	SYN	187.102.1.1	1997	191.167.1.2	21	S1	Phase6
·	10115400013.000000	TCP	PSH	187.102.1.1	1057	191.167.1.2	21	S1	Phase6
·	10113821978.000000	TCP	PSH	191.167.1.2	21	191.167.1.1	1057	T	Phase6
·	10113414114.000000	TCP	PSH	191.167.1.1	1057	191.167.1.2	21	S1	Phase6
·	10111215115.000000	TCP	PSH	191.167.1.1	1057	191.167.1.2	21	S1	Phase6

Fig.1.5.(h5%"(A<'%"./&%B(R8A'#"(#.('2%(A<37'('"'/..A&(@#8%C('#(>%(5A@7C/'%8

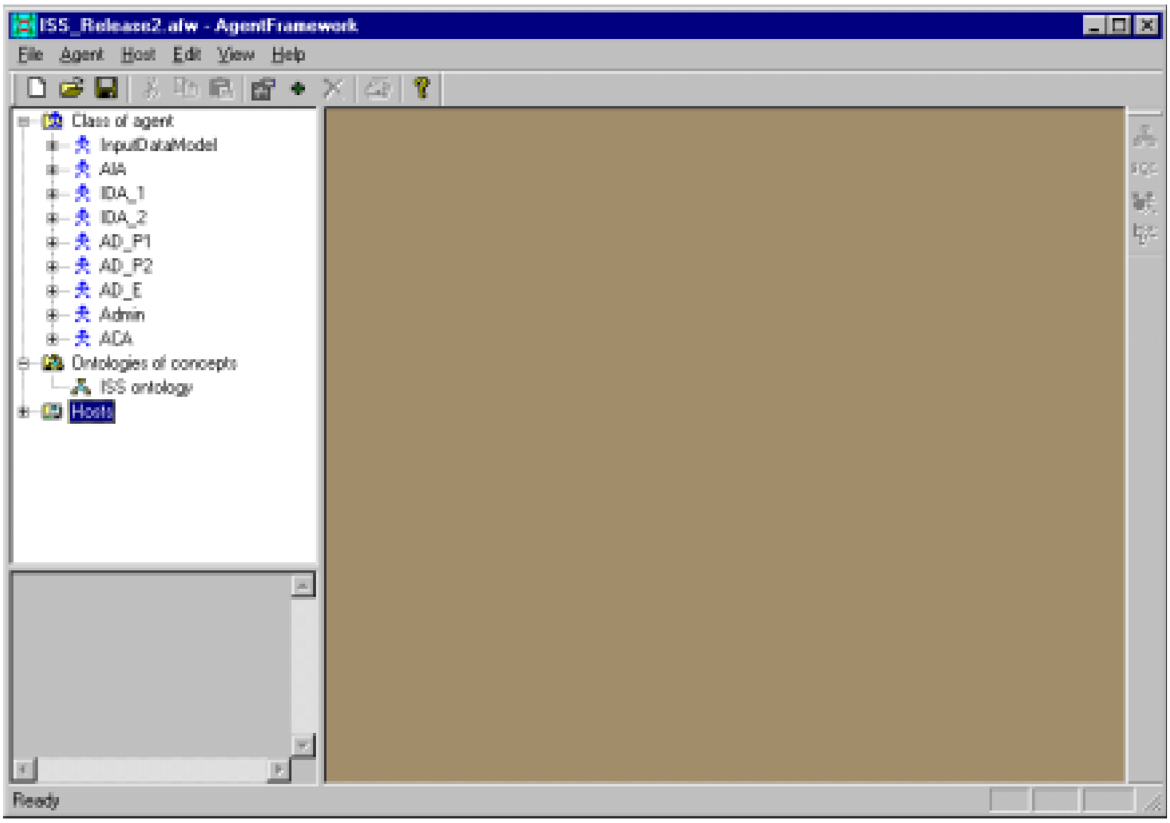


Fig.1.6.(`A5'(#.(/;%<'(&C/55%5(#.('2%(1/5%(6'789

'7<%('2%(&#<'%<'5(#.('2%(3/"'A&7C/"(*IP*=@%55/;%5E(.#"(%S/@3C%E(*IP*(/88"%55%5(#.('2%(/''/&P('/";%'5(Z2#5' #.('2%(&#@37'%"(<%'F#"P(/''/&P%8[(/<8(5#(#<4(:5(/("%57C'E('2%(A<37'('"/..A&(5A@7C/'A#<(@#8%C(A5 8%I%C#3%84(O2%(#"8%"(A<(F2A&2('2%(?!=@%55/;%5(/33%/"(A<('2%(5A@7C/'A#<(@#8%C(#.(A<37'('"/..A&(A5 8%'%"@A<%8(</'7"/CC9(/&&#"8A<;('#('2%('A@%(/55A;<%8('#('2%@4

1.7. Technology of the Case Study Development and Implementation

O2%(1/5%(6'789(#.('2%(@7C'A=/;%<'(<%'F#"P(5%&7"A'9(595'%@(8%5&"A>%8(A<('2%(3"%IA#75 5%&'A#<5(F/5(8%I%C#3%8(/<8(A@3C%@%<'%8(/5(/<(/33CA&/'A#<(#.('2%(5#.'F/"%('##C(\D7C'A=/;%<' 695'%@(M%I%C#3@%<'(bA'\(ZD:6Mb[4(:7'2#"5(#.('2A5(J%3#"'(8%I%C#3%8('2A5(5#.'F/"%('##C 8%5&"A>%8(A<('2%(3"%IA#75(!"#$%&'(J%3#"'(fYA<J%3)*g4

`%'(75("%@A<8('2/'(/&&#"8A<;('#('2%('%&2<#C#;9(5733#5%8(>9('2%(D:6Mb('##C('2%(5#.'F/"% A@3C%@%<'/'A#<(#.(/(@7C'A=/;%<'(595'%@(A5(&/""A%8(#7'(A<('F#(5'/;%54(:'('2%(.A"5'(5'/;%('2%(5#=&/CC%8 \695'%@(b%"<%C\(#.(/33CA&/'A#<(A5(8%I%C#3%8(F2%"%/5(/'('2%(5%&#<8(5'/;%(&C#<A<;(#.('2%(5/@3C%5(#. '2%(&#<&"%'%(5#.'F/"%(/;%<'5(A5(&/""A%8(#7'4(O2%<E('2%(&C#<%8(5#.'F/"%(/;%<'5(/"%(8%'/&2%8(."#@('2% 695'%@(b%"<%C(/<8(5A'7/'%8(#I%"('2%(&#@37'%"(<%'F#"P(2#5'54(V%C#F(F%(8%5&"A>%(A<(>"A%.('2% &#<'%<'5(#.('2%(F#"P(&/""A%8(#7'(A<('2%(8%I%C#3@%<'(#.('2%(695'%@(b%"<%C(#.('2%(1/5%(6'789(/<8(A< A'5(A@3C%@%<'/'A#<4

First Stage. Development of the System Kernel.

1. Designation of the agent classes of the Case Study

O2%(CA5'(#.(/;%<'(&C/55%5(&#<5'A'7'%8(/&&#"8A<;('#('2%(8%I%C#3%8(&#<&%3'7/C(@#8%C(#.('2%(1/5% 6'789(&#@3"A5%5(5%I%<(3/"'A&7C/"(&C/55%5(</@%8(:M(=RE(:M=!*E(:M=!-E(:?:E(:1:E(?M:=*E(?M:= -4(?<(/88A'A#<('F#(@#"%(&#@3#<%<'E(F2A&2(&#<&%3'7/CC9(/"%(<#'('2%(/;%<'(>7'(A@3C%@%<'%8 /&&#"8A<;('#('2%(/;%<'=#"A%<'%8('%&2<#C#;9E(/"%(?<37'(O"/..A&(D#8%C(/<8(:8@A<A5'"/'#"(Z5%% YA;4*4+[4

2. Ontology creation

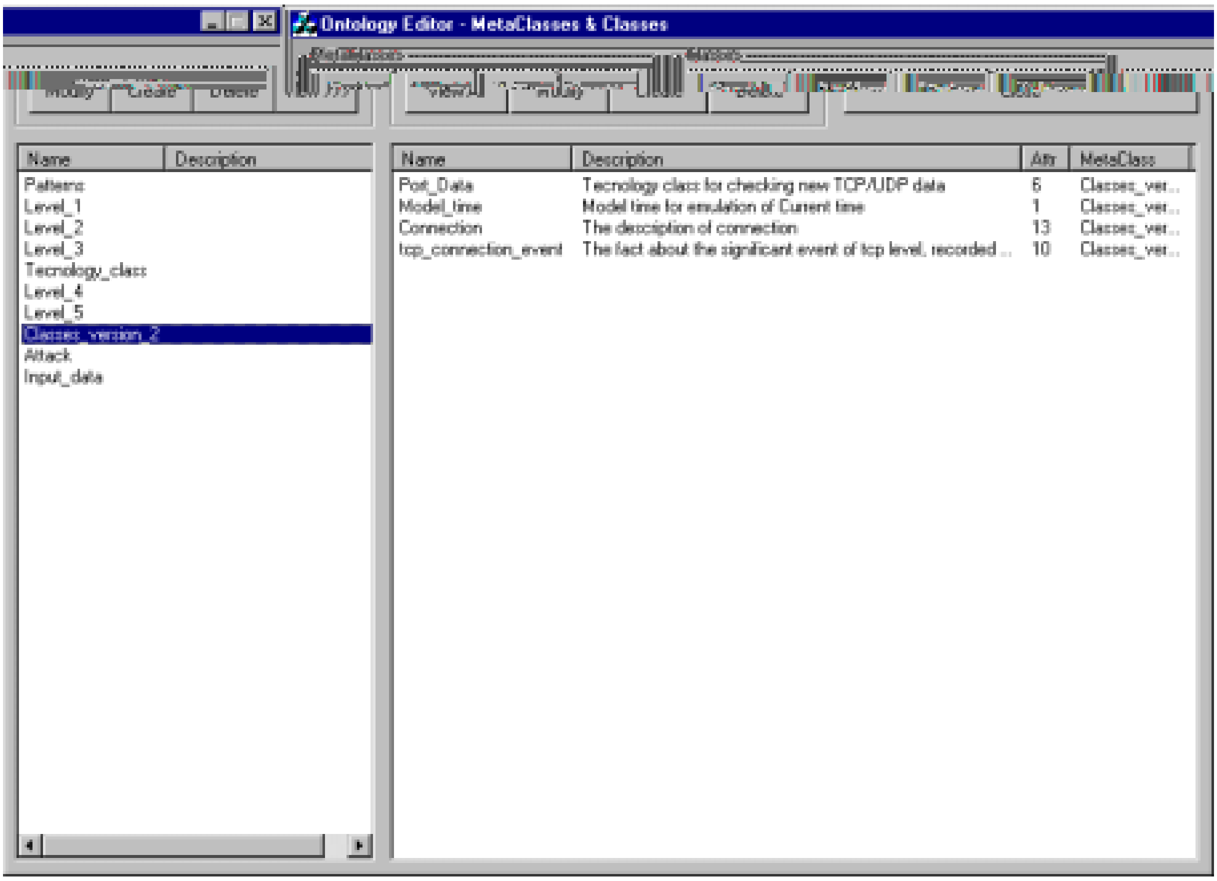
6AS(&#<&%3'5(/"%(A<&C78%8(A<'#('#3=C%I%C(8#@/A<(#<'#C#;9(Z5%%(YA;4*4Q[4(:<(%S/@3C%(#.(/(>/5A& &#<&%3'(#.('2%(1/5%(6'789(&/CC%8(\17""%<'(1#<<%&'A#<\(A5(8%5&"A>%8(A<('2%(:33%<8AS4

3. Designation scenarios to each class of the agents

?<('2%('/>C%(*4*(>%C#F('2%(CA5'(#.('2%(>%2/IA#"/C(5&%</"A#5(/&&%55A>C%(.#"(%/&2(/;%<'(A5(;AI%<4(O2% 5&%</"A#5(/"%(8%5&"A>%8(A<('%"@5(#.(#3%"/'A#<5('2/'(/"%(&/""A%8(#7'(>9(/;%<'4(O2%(&#@3C%'%(CA5'(#. 57&2(5&%</"A#5(A5(;AI%<(A<(:33%<8AS(:*4

O/>C%(*4*4(!/"'A/C(CA5'(#.(/;%<'5i(>%2/IA#"/C(5&%</"A#5

:;%<'(&C/55%5	6&%</"A#5(#.(>%2/IA#"
:M=R	• !"%3"#&%55A<;(#.(*tcp*=@%55/;%5(#.(A<37'('"/..A& • 12%&PA<;(\life time\\(#.('2%(&#<<%&'A#<5(>%C#<;A<;('#('2%(&7""%<'(&#<<%&'A#<5 • !"#&%55A<;(#.(8%'%&'%8(./&'5(A<('2%(&7""%<'(&#<<%&'A#<(8%5&"A3'A#<
:M=!*	• 12%&PA<;(#.('2%(&7""%<'(<7@>%"(#.('2%(#&&7""%<&%5(#.(\5753A&A#75\(>%2/IA#" /<8(8%'%&'A#<(#.('2%(*Port scanning* /<8 *Syn Flood* /''/&P5
:M=!-	• M%'%&'A#<(#.(*Port scanning*E(*Buffer overflow*(/<8(*Finger search*
:?:	• :7'2%<'A&/'A#<(/<8(A8%<'A.A&/'A#<
:1:	• :&&%55(&#<'"#C
?M:=*	• M%'%&'A#<(#.('2%(*Combined spoofing attack*
?M:=-	• b<#FC%8;%=>/5%8(3"#&%55A<;(#.('2%(8%'%&'%8(./&'5E(3/''%"<5E(%'&4
:8@A<A5'"/'#"	• 6'#"A<;(/<8(IA57/CA]/'A#<(#.('2%(8/'/(/>#7'(&#<<%&'A#<5(/<8(/>#7'(8%'%&'%8 /''/&P5



Name	Description
Patterns	
Level_1	
Level_2	
Level_3	
Tecnology_class	
Level_4	
Level_5	
Classes_version_2	
Attack	
Input_data	

Name	Description	Attr	MetaClass
Port_Data	Tecnology class for checking new TCP/UDP data	6	Classes_ver...
Model_time	Model time for emulation of Current time	1	Classes_ver...
Connection	The description of connection	13	Classes_ver...
tcp_connection_event	The fact about the significant event of tcp level, recorded ...	10	Classes_ver...

Fig.1.7.(O#3=C%I%C(8#@/A<(#<'#C#;9(%8A'#"

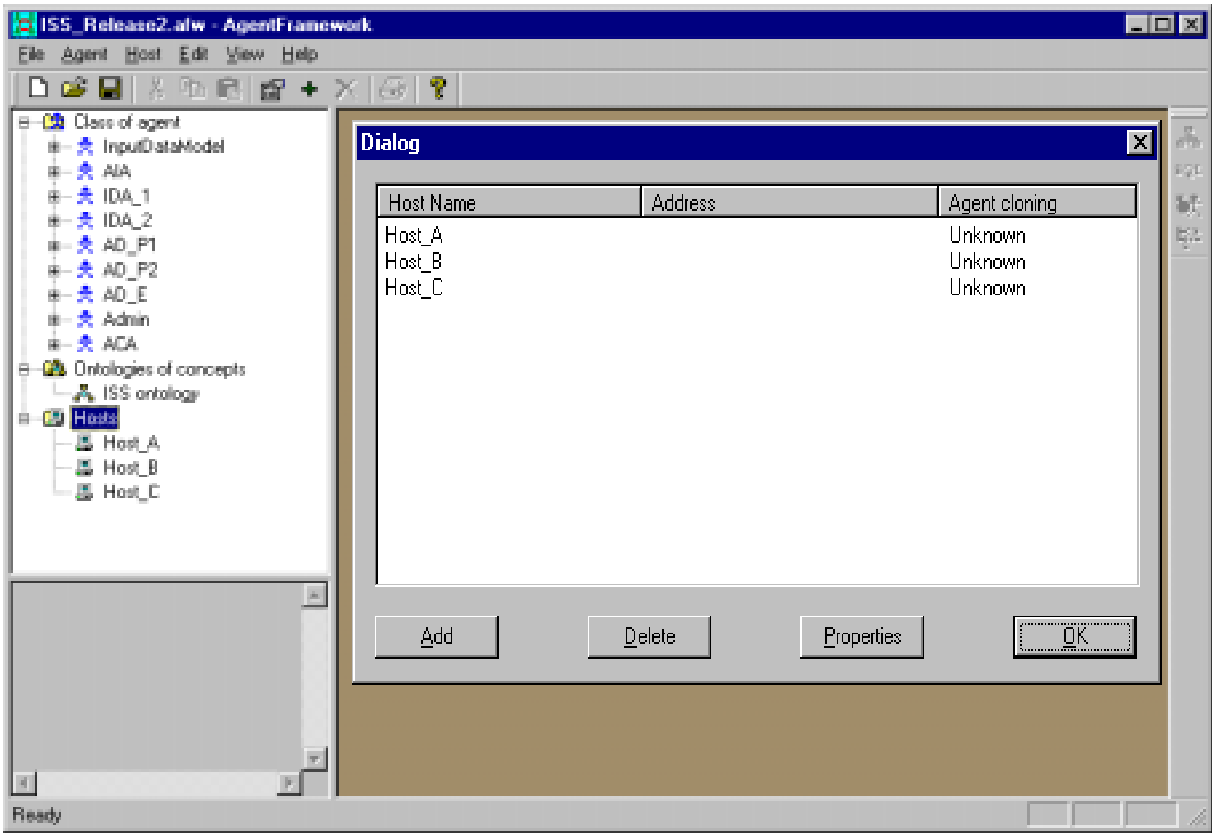
Second Stage: Cloning of the software security agents

O#(>%;A<('2%(&C#<A<;(3"#&%87"%(A'(A5("%U7A"%8('#(8%'%"@A<%('2%(</@%5(#.(2#5'5(A<(F2A&2('2%(5%&7"A'9 595'%@(A5(5733#5%8('#(>%(5A'7/'%8(ZYA;4*4,[4(?'(52#7C8(>%(<#'A&%8('2/'(A.(F%(2/I%('#(@/P%(8A5'A<&'A#< >%'F%%<('2%(</@%5(#.(2#5'5(*comprising the Case Study*(/<8('2%(</@%5(#.(*computers in which the Case Study is supposed to install*4(O2%(1/5%(6'789(A5('2%(@#8%C(#.(/(5%&7"A'9(595'%@(/<8(A'(&/< &#@3"A5%(*N* 2#5'5('#(>%(3"#'%&'%84(Y#"(%S/@3C%E(A<(#7"(&/5%(Z5%%(YA;4*4*[(A'(&#<5A5'5(#.(.#7"(2#5'5 </@%8(YE(OE(6*E(/<8(6-4

`%'(75(8%<#'%('2%(5%'(#.(/;%<'5('2/'(/&&#"8A<;('#('2%(8%I%C#3%8(1/5%(6'789(#.('2%(@7C'A=/;%<' 5%&7"A'9(595'%@(/"&2A'%&'7"%(@75'(>%(5A'7/'%8(#<(/(2#5'(j(>9(**A**Z j [4(?<(#7"(1/5%(6'789('2%(%<'A"%(5%' #.(/;%<'5('#(>%(&C#<%8(A5(**A**v**A**ZO[∪**A**ZY[∪**A**Z6*[∪**A**Z6-[4(O2A5(@#8%C(&/<(>%(A<5'/CC%8(A<(/(5A<;C%("%/C &#@37'%"E(A<('F#(#.('2%@(/<8(5#(#<(73('#(*N*.(?<(#7"(&/5%('2%(@#8%C(&/<(>%(A<5'/CC%8(#<(*R*("%/C &#@37'%"5(F2%"%(*R*∈w*E-EOEGx4(!"/&'A&/CC9E('2%(5A@7C/'%8(@#8%C(#.('2%(1/5%(6'789(F/5(A<5'/CC%8(A< '2"%%(&#@37'%"5(8%<#'%8(>%C#F(/5(K#5'=:E(K#5'=V(/<8(K#5'=14(`%'(75(&#<5A8%"('2%(5%U7%<&%(#. #3%"/'A#<('#(>%(&/""A%8(#7'(A<(87"A<;(&C#<A<;(#.('2%(5#.'F/"%(/;%<'5(/<8(A<5'/CC/'A#<('2%(1/5%(6'789 #<('2%("%/C(&#@37'%"54

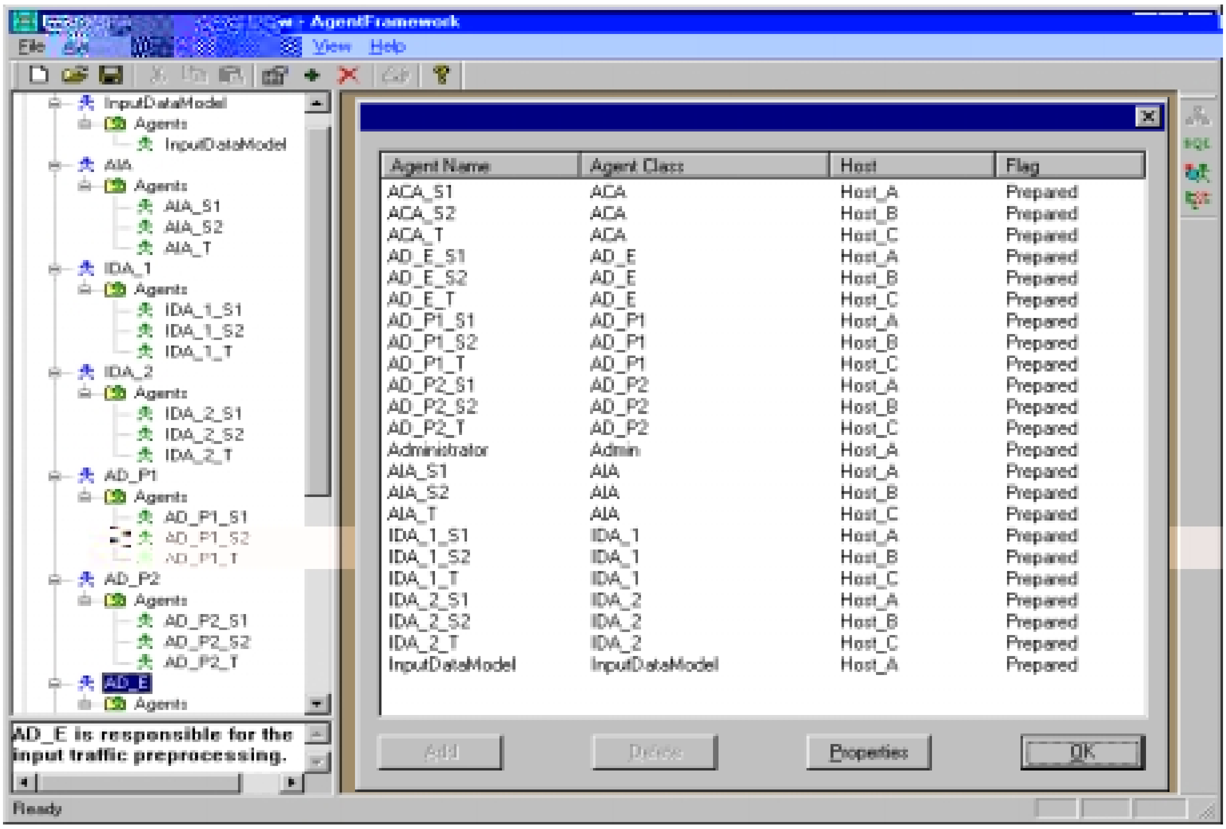
*4(M%5A;</'A#<('2%(&#@37'%"5(A<(F2A&2('2%(1/5%(6'789(FACC(>%(A<5'/CC%84(M%<#'%('2%@(/5(/>#I% K#5'=:E(K#5'=V(/<8(K#5'=14

-4(?<5'/CC/'A#<('2%(5#.'F/"%(*Agent cloning* A<(%/&2(#.('2%(/>#I%(&#@37'%"54(O2A5(5#.'F/"%(3"#IA8%5 .#"("%@#'%(/&&%55(."#@('2%(&#@37'%"(A<(F2A&2('2%(695'%@(b%"<%C(A5(A<5'/CC%8('#('2%(.AC%5(#.('2%(2#5' A<(F2A&2('2%(/;%<'(A5(A<5'/CC%84(?<(/88A'A#<E(A<(%/&2(57&2(&#@37'%"(5%I%"/C(#'2%"(5#.'F/"% &#@3#<%<'5(/"%(A<5'/CC%84(?<(3/"'A&7C/"E('2%9(/"%(&#@@7<A&/'A#<(5#.'F/"%(/<8('2%(CA>"/"9(#.(;%<%"A& 3"#&%87"%5('#(A@3C%@%<'(5&%</"A#5(#.(/;%<'i5(>%2/IA#"4



Host Name	Address	Agent cloning
Host_A		Unknown
Host_B		Unknown
Host_C		Unknown

Fig.1.8.((O2%(2#5'(</@A<;(/<8("%/C(&#@37'%"(8%5A;</'A#<(A<'%"./&%



AD_E is responsible for the input traffic preprocessing.

Agent Name	Agent Class	Host	Flag
ACA_S1	ACA	Host_A	Prepared
ACA_S2	ACA	Host_B	Prepared
ACA_T	ACA	Host_C	Prepared
AD_E_S1	AD_E	Host_A	Prepared
AD_E_S2	AD_E	Host_B	Prepared
AD_E_T	AD_E	Host_C	Prepared
AD_P1_S1	AD_P1	Host_A	Prepared
AD_P1_S2	AD_P1	Host_B	Prepared
AD_P1_T	AD_P1	Host_C	Prepared
AD_P2_S1	AD_P2	Host_A	Prepared
AD_P2_S2	AD_P2	Host_B	Prepared
AD_P2_T	AD_P2	Host_C	Prepared
Administrator	Admin	Host_A	Prepared
AIA_S1	AIA	Host_A	Prepared
AIA_S2	AIA	Host_B	Prepared
AIA_T	AIA	Host_C	Prepared
IDA_1_S1	IDA_1	Host_A	Prepared
IDA_1_S2	IDA_1	Host_B	Prepared
IDA_1_T	IDA_1	Host_C	Prepared
IDA_2_S1	IDA_2	Host_A	Prepared
IDA_2_S2	IDA_2	Host_B	Prepared
IDA_2_T	IDA_2	Host_C	Prepared
InputDataModel	InputDataModel	Host_A	Prepared

Fig.1.9.(63%&A.A&/'A#<(#.('2%(/"&2A'%&'7"%(#.('2%(@7C'A=/;%<'(5%&7"A'9(595'%@(('#(>%(&C#<%8

O4(63%&A.A&/'A#<(#.('2%(/"&2A'%&'7"%(#.('2%(@7C'A=/ ; %<'(5%&7"A'9(595'%@(&#@3"A5A< ; ('2%(5#.'F/"% / ; %<'5('#(>%(&C#<%84(O2A5(53%&A.A&/'A#<(A5(&/""A%8(#7'(FA'2A<(695'%@(b%"<%C(75A< ; ('2%("%53%&'A I % %8A'#"4(?<(./&'E(\53%&A.A&/'A#<(#.('2%(5#.'F/"%(/ ; %<'(/"&2A'%&'7"%\(A5(53%&A.A&/'A#<(#.('2%(<7@>%"(#. 5/@3C%5(#.(/ ; %<'5(#.(%/&2(&C/55(Z5%%(YA ; 4*4T[E(/55A ; <A< ; ('#(%/&2(57&2(/ ; %<'(/(7<AU7%(</@%E(3#A<'A< ; #7'(A'5(&C/55(/<8(A<8A&/'A< ; ('2%(</@%(#.("%/C(&#@37'%"(A<(F2A&2('2%("%53%&'A I %(/ ; %<'(A5(; #A< ; ('#(>% 5A'7/'%84(?<('2%(1 /5%(6'789('2%(</@%5(#.(/ ; %<'5(/"%(.#"@%8('2"#7 ; 2(&#<&/'%</'A#<(#.('2%(/ ; %<'(&C/55 /<8('2%(</@%(#.('2%(1 /5%(6'789(2#5'(A<(F2A&2(A'(A5(5A'7/'%84(Y#"(%S/@3C%E(A.(/ ; %<'i5(</@%(A5(: M=R4O '2%<('2A5(/ ; %<'(A5(#.(&C/55(R(/<8(A5(; #A< ; ('#(>%(5A'7/'%8(A<('2%(2#5'(O(#.('2%(1 /5%(6'789(@#8%C4 Y#"@/CC9E(5#.'F/"%(&#@3#<%<'(: ; %<'(&C#<A< ; (&"%/'%5('2%(.#C8%"(#<('2%("%/C(&#@37'%"(A<(F2A&2 / ; %<'(A5(5733#5%8('#(>%(A<5'/CC%8(A<(F2A&2('2%(3/""A&7C/"(5#.'F/"%(&#@3#<%<'5(#.('2%(/ ; %<'5(FACC(>% 5/ I %84

G4(O2%(.#7"'2(5'%3(A5(.A</CA]A< ; ('2%(/ ; %<'5(&C#<A< ; 4(?'(&/""A%5(#7'('F#(#3%"/'A#<54(O2%(.A"5'(#.('2%@(A5 &#39A< ; (/ ; %<'i5(P<#FC%8 ; %(>/5%5(."#@(695'%@(P%"<%C(A<('2%("%53%&'A I %(.#C8%"5(Z5%%(A'%@(0(/>#I%[4 O2%(5%&#<8(#3%"/'A#<(A5(8%5A ; </'A#<(M6_(</@%(#.(/CA/5(A<(HMV1(#.(M/'/(6#7"&%(: 8@A<A5'"/'A#<(#. 1#<'"#C(! /<%C(^ A<T , a _O4(V#'2(#.('2%5%(#3%"/'A#<5(&/<(>%(&/""A%8(#7'(%A'2%"(/7'#@/'A&/CC9(#" @/<7/CC94(?.(/<(/ ; %<'(2/5(>%%<(/C"%/89(&C#<%8('2%<('2%(.A%C8(\YC/ ; \(A<('2%("%53%&'A I %(75%"(A<'%"./&% FA<8#F('/P%5(I /C7%(\1C#<%8\(Z5%%(YA ; 4(*4T[4

1.8. Case-study Simulation: An Example of a Distributed Attack and Multi-agent System Performance

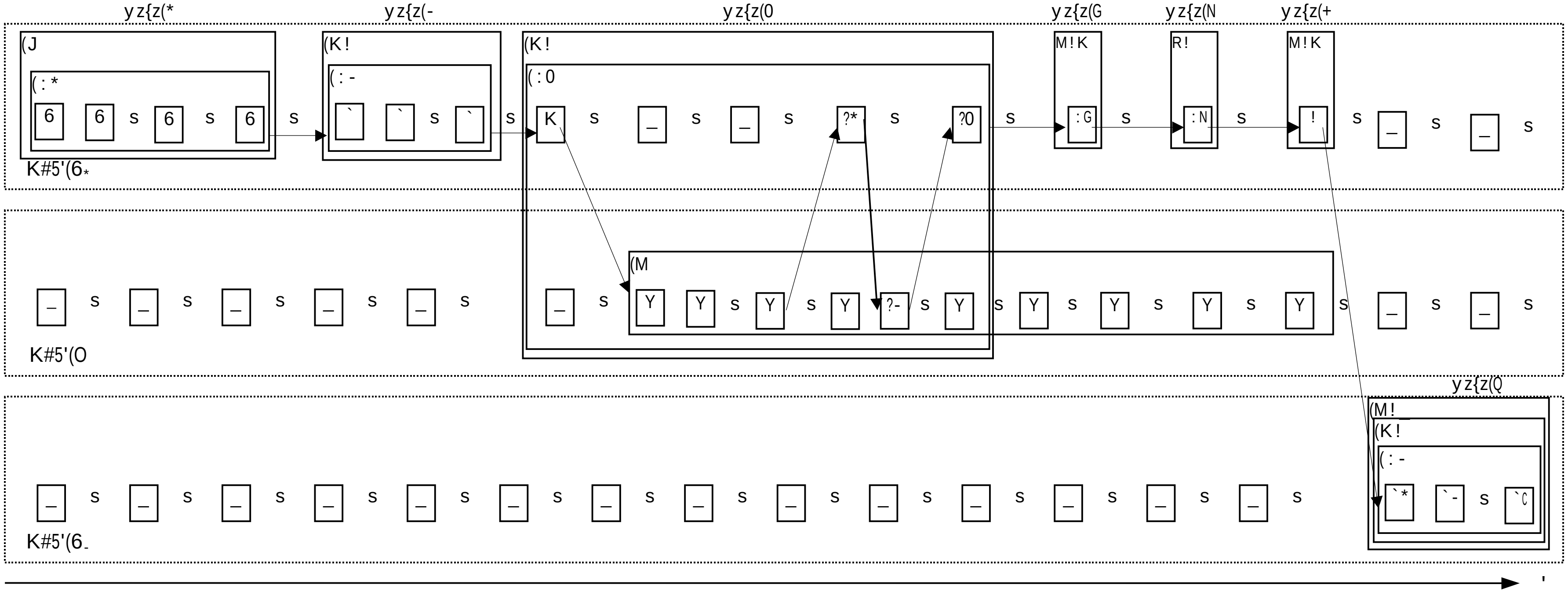
: (3/""A&7C/"(/''/&P(/ ; /A<5'(&#@37'%"(<%'F#"P(A5(5A@7C/'%8(>9(/(5%U7%<&%(#.(A<37'(*IP*=3/&P%'54 6#@%(#.('2%@(&#""%53#<8('#(<#"@/C(&#<<%&'A#<5E(#'2%"(#<%5(&#""%53#<8('#(/<(/''/&P(5A@7C/'A#<4 O2%('#'/C(C%< ; '2(#.(A<37'(*IP*=3/&P%'(5%U7%<&%(A5(#.('2#75/<85(/@#< ; (F2A&2(5% I %"/C(27<8"%85 &#""%53#<8('#(/<(/><#"@/C(75%"(/&'A I A'94(h33%"(C% I %C("/<8#@A]/'A#<=>/5%8(@%&2/<A5@(/CC#F5 5A@7C/'A< ; (8A..%"%<'(#"8%"(#.(32/5%5(#.(/''/&P54

6A@7C/'A#<(F /5(#" ; /<A]%8(#<('2%(>/5A5(#.('2%(.#CC#FA< ; (5'"/'% ; 9(#.(/''/&P%"4(?'(A5(5733#5%8 '2/'('2%(/''/&P(5#7"&%(A5('2%(@/C%./&'#"i5(2#5'(e(/<8(/''/&P(A5("%/CA]%8(/ ; /A<5'('2%(&#@37'%"(<%'F#"P 8%3A&'%8(A<(YA ; 4*4*4(Y#"(%/&2(2#5'=>/5%8(3"#'%&'A#<(595'%@(A'(A5(5733#5%8('2/'('2%(2#5'(O(A5(/(""75'%8 2#5'E(F2A&2(75%"5(2/ I %(/<(%S'%<8%8(/&&%55('#('2%("%5#7"&%5(#.('2%(2#5'(6*4(?<('2%(8% I %C#3%8(&/5% 5'789('2%(5%&7"A'9(595'%@(#.(%/&2(2#5'(&#@3"A5%5(Q(/ ; %<'5(/5(A'(A5(52#F<(A<(YA ; 4*4-4(R I %"9(2#5'(A5 3"#'%&'%8(>9('2%(@7C'A=/ ; %<'(57>595'%@(#.('2%(5/@%(/"&2A'%&'7"%(&#@3"A5A< ; (5A@AC/"(/ ; %<'5(/<8 5A@AC/"(/"&2A'%&'7"%(#.('2%A"(A<'%"/&'A#<4(O2%(#<C9(8A5'A<&'A#<(>%'F%%<(8A..%"%<'(2#5'=>/5%8(5%&7"A'9 57>595'%@5(A5(2#5'=53%&A.A&('7<A< ; (#.(/ ; %<'5i(/''"A>7'%54(O2%('#'/C(<7@>%"(#.(/ ; %<'5(#.('2%(<%'F#"P 5%&7"A'9(595'%@(A5(- , 4

^ A'2A<(5A@7C/'%8(/''/&P(/(@/C%./&'#"('/" ; %'(A5('#(; %'(7</7'2#"A]%8(/&&%55('#('2%("%5#7"&%5(#. '2%(2#5'(6*4(O2%(@/C%./&'#"(A5(; #A< ; ('#(/&'(\A<8A"%&'C9\E(A4%4(2%(75%5('2%(/&&%55(&2/A<(6*oOo6*E &#<5A8%"A< ; ('2%(2#5'(6*(/<8(O(/5('2%(A<'%"A@('/" ; %'54(?'(52#7C8(>%(<#'A&%8('2/'('/C'2#7 ; 2('2%(3/""A&7C/" 32/5%5(#.(/''/&P(/"%(8%'%"@A<%8(>9('2%(&#@3#<%<'5(#.('2%(@7C'A=/ ; %<'(<%'F#"P(5%&7"A'9(595'%@E('2% &#<<%&'A#<(FA'2(@/C%./&'#"(A5(<#'(>"%/PA< ; (A<(% I %<(A.(/<(/''/&P(2/5(/C"%/89(>%%<(5753%&'%8(#" "%&# ; <A]%84(O2%("%/5#<(A5('#(A< I #C I %(A<(&##3%"/'A#<(/5(@/<9(/5(3#55A>C%(&#@3#<%<'5(#.('2%(5%&7"A'9 595'%@4(?'(52#7C8(>%(<#'A&%8('2/'(A<("%/C=CA.%(5A'7/'A#<('2A5(/557@3'A#<(&#""%53#<85('#('2%(&/5%(F2%< A'(A5(<%&%55/"9('#(>%&#@%(@#"%(A<.#"@%8(/>#7'('2%(@/C%./&'#"(/<8(2A5(37"3#5%54

6&%</"A#(#.('2%(5A@7C/'%8(/''/&P(A5(8%3A&'%8(A<(YA ; 4*4*L4(?'(A5("%3"%5%<'%8(/5(/('%@3#"/C(% I %<' 8A/ ; "/@(A<(F2A&2(57>=5%U7%<&%5(#.('2%(/''/&P(; "#73%8(/&&#"8A< ; ('#('2%(32/5%5(#.('2%(/''/&P 8% I %C#3@%<'4(O2%(/''/&P(A5(53%&A.A%8(A<('F#(C% I %C54(?<('2%(C#F=C% I %C(/''/&P(53%&A.A&/'A#<(A'(A5 "%3"%5%<'%8(A<('%"@5(#.('""/..A&(% I %<'54(O2%(% I %<'5(#.(<#"@/C(/&'A I A'9(/"%(@/"P%8(A<5A8%(>9(59@>#C \ _ \4(O2%(5A ; <A.A&/<'(% I %<'5(&#""%53#<8A< ; ('#('2%(@/C%./&'#"(/&'A I A'9(/"%(@/"P%8(>9(#'2%"(59@>#C54

?<(YA ; 4*4*L('2%(733%"=C% I %C(/''/&P(5&%</"A#(#"%3"%5%<'%8(>9('2%(5%U7%<&%(#.('2%(\5A< ; C%=32/5%\ /''/&P54(R/&2(57&2(/<(/''/&P(&#""%53#<85('#(/(57>=5%U7%<&%(#.(% I %<'5(52/3%8(>9('2%("%&'/< ; 7C/"4 H<%(&/<(5%%('2/'(@/C%./&'#"('""A%5('#(/&2A% I %(2A5('/" ; %'5(A<(5% I %<(32/5%54(O2%5%(32/5%5(Z\5A< ; C%= 32/5%(/''/&P5\[(/"%(/5(.#CC#F5B



Particular events:(6E s E6(o(6 j _(o(3/&P%'5(Z.#"(6 j _=5&/<<A<;[E(`E s E`(o(C#;A<(%I%<'5E(&#""%53#<8A<;('#('2%(/''%@3'5(#.(/(3/55F#"8(;7%55A<;E(K(o(%I%<'(K/<852/P%("%&#<</A55/<&%E YE s EY(o(6 j _=3/&P%'5(Z.#"(6 j _(YC##8[E(?*(o(%I%<'5(&#""%53#<8A<;('#('2%(A@A'/'A#<(#.('2%(.A"5'(32/5%(#.(2/<852/PA<;E(?-(o(&#<.A"@/'A#<(3/&P%'(."#@('2%(2#5'(6*E(?0(o(%I%<'(&#""%53#<8A<; '#('2%(A@A'/'A#<(#.('2%('2A"8(32/5%(#.('2%(2/<852/PA<;E(!(o(/&&%55('#('2%(3/55F#"8(.AC%(#<(>%2/C.(#.('2%(:8@A<A5'"/'#"E(_(o3/&P%'(#.(<#"@/C(""/..A&k

*Attacks*B(:*(o(3#"'(5&/<<A<;E(:-(o(&#<<%&'A#<(/<8(3/55F#"8(;7%55A<;E(M(o(M#6(Z6 j _(YC##8[(/''/&PE(:0(o(&#@>A<%8(53##.A<;=/''/&PE(:G(o(7</7'2#"A]%8(/&&%55('#('2%(.AC%E(:N(o(V7..%" #I%".C#F(/''/&Pk

X%<%"/CA]%8(/''/&P(5&%</"A#5B(Jo"%&#<</A5/<&%E(K!o2#5'(3%<%'"/'A#<E(R!=%5&/C/'A<;(3"AIAC%;%5E(M!Ko8%%3A<;(3%<%'"/'A#<(A<'#('2%(2#5'E(M!_o8%%3A<;(3%<%'"/'A#<(('2"#7;2(<%'4

Fig.1.10.(OA@%=#"8%"%8(8A/;"/@(#.('2%(3/"'A&7C/"(/''/&P(5&%</"A#

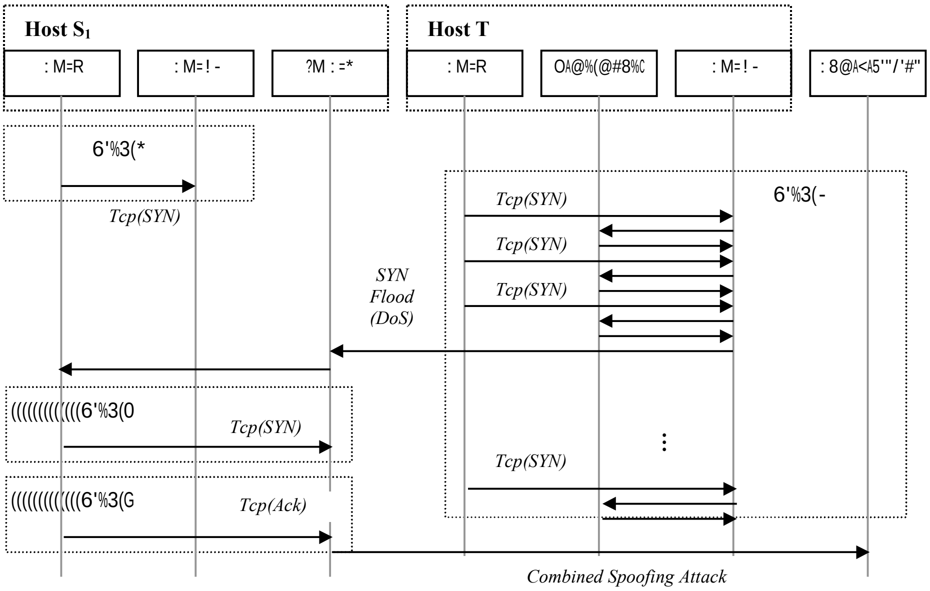


Fig.1.11.(: ;%<'5i(A<'%"/&'A#<(87"A<;(3"#&%55A<;(#.('2%(*Combined Spoofing Attack*

*4(6&/<<A<;(#.('2%(3#"'5(#.('2%(2#5'(6*4

-4(: ''%@3'5(#.(&#<<%&'A#<(#<('2%(2#5'(6*('#(/&&%55('#(A'5(.'3(#"('%C<%'(5%"I A&%5(75A<;(I/"A#75(5#7"&% *IP*=/88"%55%5(/<8(;7%55A<;(3/55F#"84(?'(A5(5733#5%8('2/'('2A5(/''/&P(A5(7<57&&%55.7C4

O4(J%/CA]/'A#<(#.('2%(&#@>A<%8(53##.A<;(/''/&P4(?<(;%<%"/C(F#"85('2%(5&%</"A#(#.('2A5(/''/&P(F/5 8%5&"A>%8(A<(5%&'A#<(*4+4(`%'(75(53%&A.9(A'5(3/"'A&7C/"("%/CA]/'A#<(A<(&#<'%S'(#.('2%(1/5%(6'789 &#@3"A5A<;(.#7"(2#5'5(YE(OE(6*(/<8(6-4(O2%(/''/&P(A5(8A"%&'%8(/;/A<5'(2#5'(6*('2"#7;2(2#5'(O4(?' &#<5A5'5(#.(.#7"(5'%35B

Z/[(D/C%./&'#"(&#<5'A'7'%5(&#<<%&'A#<(."#@(2#5'(e(FA'2(2#5'(6*(/<8("%&%A I%5(A<A'A/C(?6_5* <7@>%"(#.(&#<<%&'A#<(\eo6*\4(O2A5(<7@>%"(/CC#F5('#(@/C%./&'#"('#(&/C&7C/'%('2%(A<A'A/C(<7@>%" #.E(?6_5-(&#<<%&'A#<(\6*oO\4

Z>[(D/C%./&'#"(e(&#@3"#@A5%5('2%(2#5'(O('2"#7;2(8A"%&'%8(5'#"@(#.(@%55/;%5(Z6 j _=.C##8[('275 A@3C%@%<'A<;(*Denial of Service*\(/''/&P4

Z&[(D/C%./&'#"(e(%5'/>CA52%5(&#<<%&'A#<(FA'2('2%(2#5'(6*(\#<(>%2/C.\(#.('2%('"75'%8(2#5'(O(/<8 &/C&7C/'%8(A<A'A/C(<7@>%"(?6_5-(#.('2%(&#<<%&'A#<(\(6*oO\E(6*(5%<85(\"%3C9(#.('2%(2#5'(O\('# &#<.A"@(%5A5'%<&%(#.('2%(&#<<%&'A#<(FA'2('2%(2#5'(6*(FA'2(/55A;<%8(A<A'A/C(<7@>%"?6_5-4

Z8[(D/C%./&'#"(e(3#55%55A<;(>9('2%(&#<<%&'A#<(<7@>%"(?6_5-("%3CA%5('#('2%(2#5'(6*(A<5'%/8(#. '2%(2#5'(O('275(;%''A<;(5A<;C%(5A8%(&#<<%&'A#<(FA'2('2%(2#5'(6*4(?<('2%(5A@7C/'A#<(3"#&%87"%(A' F/5(5733#5%8('2/'('2A5(/''/&P(F/5(57&&%55.7C4

G4(: ''%@3'5('#(;%'('2%(<#<=/7'2#"A]%8(/&&%55('#('2%(.AC%5(#.('2%(2#5'(6*(Z7<57&&%55.7C[4

N4(V7..%"(#I%".C#F(/''/&P('#(>##5'(/&&%55("A;2'5('#('2%(2#5'(6*("%57C'A<;(A<(;%''A<;(/&&%55('#('2% 3/55F#"8(.AC%(#.('2%(2#5'(6*(Z57&&%55.7C[4

+4(J%/8A<;('2%(3/55F#"85(/<8(;%''A<;(/&&%55('#('2%(.AC%5(#.('2%(2#5'(6-(Z57&&%55.7C[4

Q4(1#<<%&'A#<('#('2%(.'3(#"('%C<%'(5%"I A&%(#.('2%(2#5'(6-(Z57&&%55.7C[4

6A@7C/'A#<(#.('2A5(&#@>A<%8(/''/&P(5'/"'5(FA'2("7<<A<;(#.('2%(?<37'(O"/..A&(D#8%C(5#.'F/"%E F2A&2(A5(A@A'/'A<;('2%(5%U7%<&%(#.('2%(A<37'(*IP*-3/&P%'54(O2%5%(3/&P%'5(/"%(5%<'('#('2%(2#5'5(6-(/<8 O4(`%'(75(&#<5A8%"(2#F('2%(5%&7"A'9(595'%@(/;%<'5(#3%"/'%(/<8(A<'%"/&'(87"A<;('2%(8%5&"A>%8(/''/&P 8%I%C#3@%<'4(?<37'("'/..A&(A5(3"%3"#&%55%8(>9('2%(/;%<'=8%@#<(: M=RE(F2A&2("%=/88"%55%5('2% "%57C'A<;(@%55/;%5('#('2%(53%&A/C]%8(/;%<'=8%@#<5(: M=! *(/<8(: M=! -4(: '('2%(.A"5'(32/5%(#.('2% /''/&P('2%(/;%<'=8%@#<(: M=! -(#.('2%(2#5'(6*(A5(3C/9A<;('2%(C%/8A<;("#C%4(O2%(5%&#<8(32/5%(A<I#CI%5 /;%<'5(: ? : (#.('2%(5/@%(2#5'4(O2%('2A"8(32/5%(A5(@#<A'#"%8(>9('2%(/;%<'5(: M=! -(/<8(?M : *(#.('2% 2#5'(6*(/<8(/;%<'(: M=! -(#.('2%(2#5'(O4(M7"A<;('2%(.#7"'2(32/5%('2%(/;%<'5(: ? : (/<8(: 1 : (#.('2%

2#5'(6*(/'"%(#3%"/'A<;4(: ;%<'(: M=!*(#.('2%(2#5'(6*(8%'%"@A<%5('2%(<%S'(32/5%(#.(/''/&P4(M7"A<;('2% 5AS'2(32/5%('2%(/;%<'5(: 1 : (/<8(?M : -(#.('2%(2#5'(6*(/'"%(#3%"/'A<;4(M7"A<;('2%(.A</C(32/5%(#.(/''/&P '2%(/;%<'5(: ? : (/<8(: 1 : (#.('2%(2#5'(6-(/'"%(F#"PA<;4(: <(%S/@3C%(#.(A<'%"/&'A#<(5&%</"A#(#.('2% 5%&7"A'9(/;%<'(&#@@7<A'9(A5(8%3A&'%8(A<(YA;4*4**4(?'(&#""%53#<85('#('2%('2A"8(32/5%(#.(/''/&P 8%I%C#3@%<'(F2%<('2%(@/C%./&'#"(A5("%/CA]A<;(/(&#@>A<%8(53##.A<;(/''/&P4

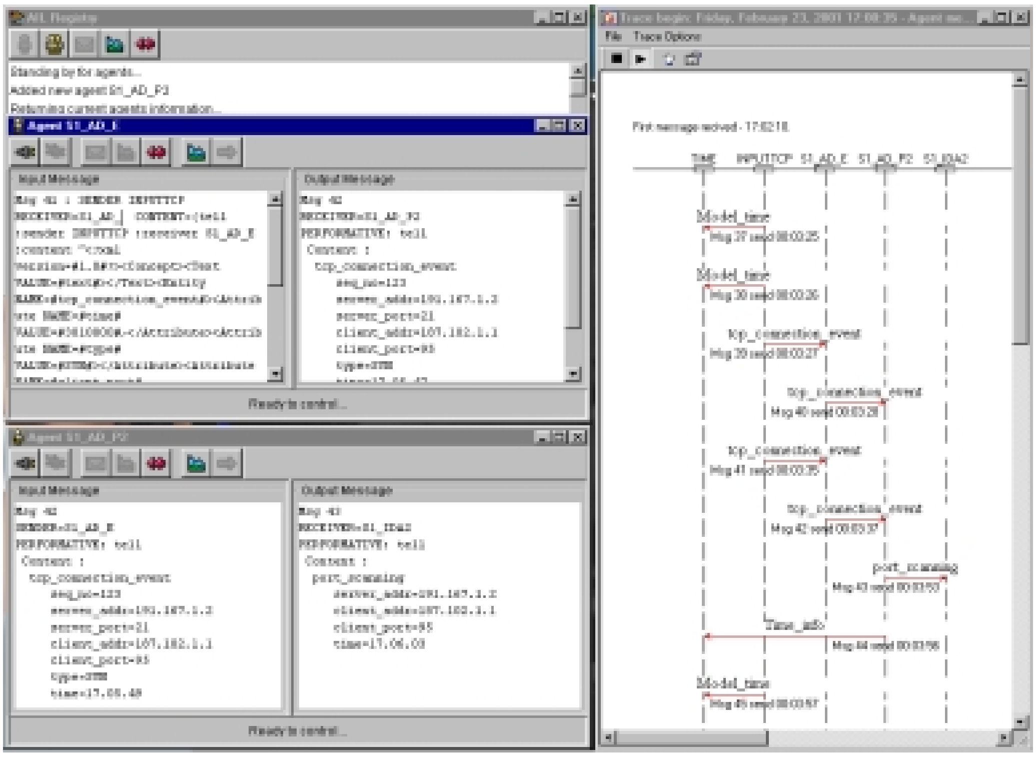
`%'(75(&#<5A8%"('2%(/;%<'i5(A<'%"/&'A#<5(87"A<;('2%('2A"8(32/5%(#.('2%(/>#I%=8%5&"A>%8(/''/&PE F2A&2(&#""%53#<85('#('2%(&#@>A<%8(53##.A<;(/''/&P(ACC75'"/'%8(A<(YA;4*4**4

J%@A<8('2/'('2A5(/''/&P(A5(&/""A%8(#7'(A<(.#7"(5'%35(Z5%%(/>#I%[4(O2%(.A"5'(5'%3(A5(%5'/>CA52@%<' #.('2%(*tcp*=&#<<%&'A#<(#.('2%(@/C%./&'#"i5(2#5'(e(FA'2('2%(2#5'(6*(/<8("%&%AIA<;(A<A'A/C(<7@>%"(#.('2% &#<<%&'A#<4(O2%(5%&#<8(5'%3(A5("%/CA]/'A#<(#.('2%(*Denial of Service*\(/''/&P(/;/A<5'('2%(2#5'(O4(O2% '2A"8(5'%3(A5(%5'/>CA52@%<'(#.('2%(*tcp*=&#<<%&'A#<(#.('2%(2#5'(e(FA'2('2%(2#5'(6*(\#<(>%2/C.\(#.('2% 2#5'(O(.#CC#F%8(>9(5%<8A<;(#.('2%(&#<.A"@/'A#<("%&%A3'(."#@('2%(2#5'(6*('#('2%(2#5'(O4(YA</CC9E('2% .#7"'2(5'%3(A5(5%<8A<;(."#@('2%(2#5'(e('2%("%3C9('#('2%(2#5'(6*(\#<(>%2/C.\(#.('2%(2#5'(O4(`%'(75 &#<5A8%"('2%(8%'/AC5(#.('2A5(/''&P(/<8(/;%<'(A<'%"/&'A#<(ACC75'"/'%8(A<(YA;4*4**4

At the first step '2%(2#5'(e(%5'/>CA52%5('2%(*tcp*=&#<<%&'A#<(FA'2('2%(2#5'(6*4(?.('2%(&#<<%&'A#< FA'2('2%(2#5'(6*(A5(%5'/>CA52%8('2%(*tcp*=@%55/;%(/55A;<%8(.C/;(6 j _(A5(5%<'(."#@('2%(/;%<'=8%@#< : M=R(#.('2%(2#5'(6*('#('2%(/;%<'(: M=!*(Z5%%(YA;4*4**[4?'(A5(A@3%"/'AI%('2/'(57&2(/(@%55/;%('#(/(2#5' @75'(>%(.#CC#F%8(>9('2%(<%S'(5A@AC/"(@%55/;%(/55A;<%8(.C/;(: 1 b4(?.(57&2(/(@%55/;%(A5(<#'(>%A<; "%&%AI%8(>9('2%(2#5'(6*(/<8E('2%"%.#"%E(<#'("%&%AI%8(>9(A'5(/;%<'(: M=!*('2%<('2%(C/''%"(@/P%5 &#<&C75A#<('2/'('2A5(*tcp*=&#<<%&'A#<(A5(\2/C.=#3%<\4

At the second step('2%(2#5'(O("%&%AI%5('2%(5%U7%<&%(#.('2%(A<37'(*tcp*=@%55/;%5(/55A;<%8(>9('2% .C/;(6 j _4(O2%5%(@%55/;%5(3"#&%55%8(>9(/;%<'(: M=R(A5(.#"F/"8%8('#('2%(/;%<'(: M=!*4(?.(57&2(/ @%55/;%(A5("%&%AI%8(>9('2%(/;%<'(: M=!*('"%%('A@%5(/'(/("7<('2%<('2%(C/''%"(&#<&C78%5('2/'('2A5 /&'AIA'9(A5(5753A&A#75(/<8(&/<(>%('2%(*SYN flood*(/''/&P(#.('2%(*Denial of service*(&C/554(O2A5(&#<&C75A#< />#7'(5753A&A#75(>%2/IA#"(A5(5%<'('#('2%(A<'"75A#<(8%'%&'A#<(/;%<'5(?M : *(#.('2%(#'2%"(2#5'54(?< 3/"'A&7C/"E('2%(/;%<'(?M : *(#.('2%(2#5'(6*(("%&%AI%5(57&2(/(@%55/;%4

At the third step('2%(/;%<'=8%@#<(: M=R(#.('2%(2#5'(6*(5%<85('2%(@%55/;%('#(A'5(A<'"75A#< 8%'%&'A#<(/;%<'(?M : *('#(A<.#"@(A'(/>#7'("%&%AIA<;('2%(@%55/;%(/55A;<%8(.C/;(6 j _(."#@('2%(2#5'(O4



AIL Registry

Standing by for agents...
Added new agent S1_AD_P3
Returning current agents information...

Agent S1_AD_E

Input Message

```
Msg 41 : SENDER INPUTTCP
RECEIVER=S1_AD_E  CONTENT=(tell
:sender INPUTTCP :receiver S1_AD_E
:content "<xml
version=#1.0#><Concept><Text
VALUE=#text#></Text><Entity
NAME=#tcp_connection_event#><Attrib
ute NAME=#time#
VALUE=#061080#></Attribute><Attrib
ute NAME=#type#
VALUE=#SYN#></Attribute><Attribute
```

Output Message

```
Msg 42
RECEIVER=S1_AD_P2
PERFORMATIVE: tell
 Content :
  tcp_connection_event
     seq_no=123
     server_addr=191.167.1.2
     server_port=21
     client_addr=167.182.1.1
     client_port=85
     type=SYN
```

Ready to control...

Agent S1_AD_P2

Input Message

```
Msg 42
SENDER=S1_AD_E
PERFORMATIVE: tell
 Content :
  tcp_connection_event
     seq_no=123
     server_addr=191.167.1.2
     server_port=21
     client_addr=167.182.1.1
     client_port=85
     type=SYN
     time=17.05.48
```

Output Message

```
Msg 43
RECEIVER=S1_IDA2
PERFORMATIVE: tell
 Content :
  port_scanning
     server_addr=191.167.1.2
     client_addr=167.182.1.1
     client_port=85
     time=17.06.03
```

Ready to control...

Trace begin: Friday, February 23, 2001 17:08:35 - Agent me...

Fig.1.12.(!"A<'#7'(#.('2%(IA57/C(A<'%"./&%("%3"%5%<'A<;(/;%<'5i(A<'%"/&'A#<

: ;%<'(?M : *($#A<5('2A5(./&'(FA'2('2%(./&'(A<.%'""%8(/'('2%('2A"8(5'%3(/<8(75A<;(A'5(P<#FC%8;%(>/5% &#<&C78%5('2/'(/(5753A&A#75(>%2/IA#"(A5('/PA<;(3C/&%(/'('2%(2#5'(A<37'4(?'(&C/55A.A%5('2A5(>%2/IA#"(/5 *possibly, unknown user imitates tcp-connection with the host S_1 on behalf of the trusted host T*\4

At the fourth step /;%<'=8%@#<(#.('2%(2#5'(6*(5%<85('2%(@%55/;%('#('2%(A<'"75A#<(8%'%&'A#< /;%<'(?M : *(#.('2%(5/@%(2#5'('2/'(A'("%&%AI%8(@%55/;%(FA'2('2%(.C/;(: 1b(."#@('2%(2#5'(O4(?M : * A<.%"5('2/'('2%(&#@>A<%8(63##.A<;(: ''/&P(A5('/PA<;(3C/&%4

H<%(@#"%(%S/@3C%(#.(/;%<'(A<'%"/&'A#<(A5(;AI%<(A<(YA;4*4*-4(O2A5(.A;7"%(A5(3"A<'#7'(#.(/(75%" IA57/C(A<'%"./&%(FA<8#F(3"%5%<'A<;(/;%<'(A<'%"/&'A#<(87"A<;('2%(3#""(5&/<<A<;(/''/&P(3"#&%55A<;4 `%.'=2/<8(3/A"(#.(FA<8#F5(>#'2('#3(/<8(>#''#@("%.C%&'5(/(3/A"(#.("%&#"85(#.('A@%=C#;(.AC%5(#.(/;%<'5 : M=R(/<8(: M=!-(#.('2%(2#5'(6*(F2A&2(A<'%"/&'(/'('2A5(5'%3(#.(#3%"/'A#<(IA/(%S&2/<;%(#.(@%55/;%5))(G*oG04(O2A5(A<'%"./&%(8%3A&'5('2%(&#<'%<'(#.(A<37'(/<8(#7'37'(@%55/;%5(A<(52#"'(#"(A<(.7CC <#'/'A#<54(_#'A&%('2/'(.7CC(<#'/'A#<(ZA<37'(@%55/;%()G*(#.(/;%<'(: M=R[(&#""%53#<85('#(/(@%55/;% &#<'%<'("%3"%5%<'%8(A<(eD`(C/<;7/;%4(O2%("A;2'=2/<8(/"%/(#.(YA;4*4*-(IA57/CA]%5('2%(3"#&%55(#.('2% /;%<'(@%55/;%(%S&2/<;%(A<('A@%=#"8%"%8(@#8%4(67&2(IA57/CA]/'A#<(A5(/(.7<&'A#</C'9(#.(/(5#.'F/"% &#@3#<%<'(&/CC%8(*Tracer.*

O2%("%57C'5(#.('2%(1/5%(6'789(3%".#"@/<&%E(A4%4('2%("%57C'5(#.(/''/&P(/<8(5753A&A#75(>%2/IA#" 8%'%&'A#<E(/"%("%3"%5%<'%8(IA57/CC9(#<('2%(53%&A/C(8A/;"/@4(O2A5(8A/;"/@(8%3A&'5('2%('A@%=#"8%"%8 5%U7%<&%5(#.('2%(8%'%&'%8(5A;<A.A&/<'(%I%<'54(O2A5(8A/;"/@(A5(/(&#@3#<%<'(#.('2%(75%"(A<'%"./&% &/CC%8(A<(YA;4*4-(\ : 8@A<A5'"/'#"\4(: <(%S/@3C%(#.(57&2(/(8A/;"/@(A5(;AI%<(A<(YA;4*4*04(?'(3"%5%<'5 3/'"A&7C/"(./&'5('2/'(/"%('2%(%IA8%<&%5(#.(/''/&P5(/;/A<5'(&#@37'%"(<%'F#"P4(O2A5(A<.#"@/'A#<(A5 "%.C%&'%8(A<('2%(733%"(/"%/(#.('2%(8A/;"/@(/<8(3"%5%<'%8(>9('2%(&#C#"%8(/<8(8%5A;<%8("%&'/<;7C/"54 ?<('2%(C%.'=2/<8(/"%/('2%(C%;%<8(%S3C/A<A<;(@/33A<;(*color*\=*evidences of attack*\(A5(8%3A&'%84

?'(A5(F%CC(P<#F<('2/'(3/'"A&7C/"(./&'5(&/<(>%(%IA8%<&%5(#.(/(&#@>A<%8(8A5'"A>7'%8(/''/&P /;/A<5'(&#@37'%"(<%'F#"P4(O2%(5/@3C%(#.(57&2(/<(/''/&P(F/5(;AI%<(/>#I%(F2%<('2%('2A"8(32/5%(#. '2%(@/C%./&'#"i5(5&%</"A#(#.(/''/&P(F/5(8%5&"A>%84(O2%(8%'%&'%8(32/5%5(#.(/(&#@>A<%8(/''/&P(/"% 8%3A&'%8(A<('2%(C#F="A;2'=2/<8(/"%/(#.('2%(8A/;"/@4(h5%"(A<'%"./&%(/CC#F5(@/"PA<;(Z>9(53%&A/C ""/&%"9[('2%(5%'(#.(./&'5('2/'(&#""%53#<85('#('2%(%IA8%<&%5(#.('2%(5/@%(/''/&P4

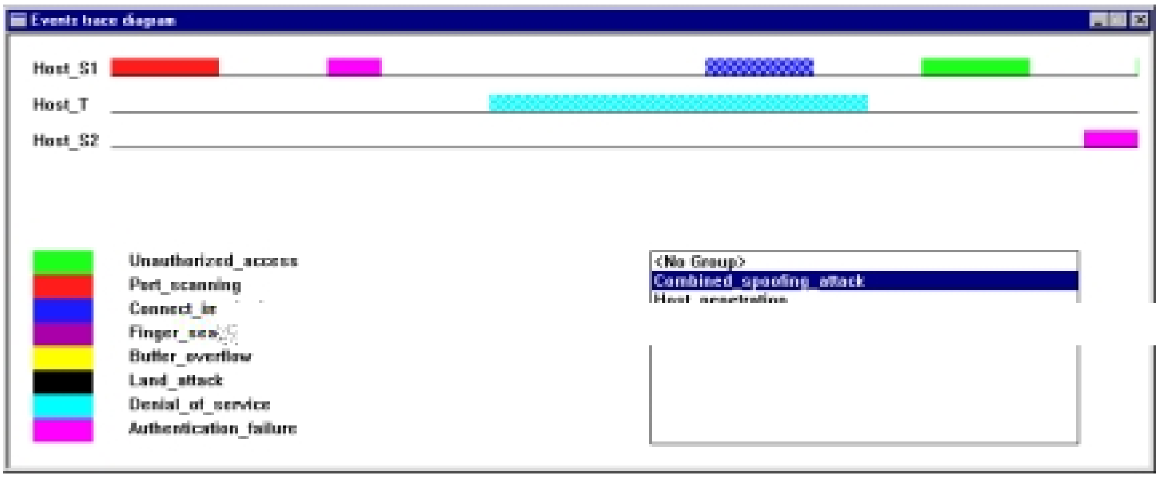


Fig.1.13.(h5%"(A<'%"./&%(.#"(/</C95A5(#.('2%("%57C'5(#.('2%(1/5%(6'789

1.9. Conclusion of Chapter 1

: 5(/("7C%E(8%I%C#3@%<'(#.(/(8A5'"A>7'%8(/''/&P(&/<(/..%&'(5%I%"/C(2#5'5(&#@3"#@A5A<;(/
<7@>%"(#.('2%@(/'('2%(5/@%('A@%4(D/C%./&'#"5(&/<(&##3%"/'%(FA'2A<(/<(/''/&P(A<(57&2(/(F/9(A<
F2A&2(/(3/"'A&7C/"(@/C%./&'#"(/''/&P5(/(5A<;C%(2#5'('275(@/5PA<;('2%(&#@>A<%8(8A5'"A>7'%8(</'7"%(#.
/<(/''/&P4(: (&%<'"/CA]%8(5%&7"A'9(595'%@(52#7C8(>%('##(\2%/I9\('#(3"#&%55('2%(%<'A"%(>/'&2(#.(C/";%=
5&/C%(8/'/(/>#7'(3"%2A5'#"9(/<8(&7""%<'(5'/'%5(#.(@/<9(&#<&7""%<'(&#<<%&'A#<5(#.(@/<9(2#5'54
6A@7C/'A#<(#.('2%(&/5%(5'789(8A53C/9%8(/(<7@>%"(#.(/8I/<'/;%5(#.(@7C'A=/;%<'(/"&2A'%&'7"%(.#"
3"#'%&'A#<(#.(/(&#@37'%"(<%'F#"P(/;/A<5'(8A5'"A>7'%8(/''/&P54(O2%(@#5'(5A;<A.A&/<'(#<%(A5(/
&/3/>ACA'9(#.(&#@3/"/'AI%C9(\CA;2'\(&#@3#<%<'5(#.(/(@7C'A=/;%<'(5%&7"A'9(595'%@('#(&##3%"/'%4(: '
3"%5%<'('2%(#<C9(F/9('#(8%'%&'(%..A&A%<'C9(/(8A5'"A>7'%8(/''/&P(/;/A<5'(/(&#@37'%"(<%'F#"P(A5(/
&##3%"/'A#<(#.(5%&7"A'9(5#.'F/"%(%<'A'A%5(Z/;%<'5[(8A5'"A>7'%8(#I%"('2%(2#5'5(#.('2%(<%'F#"P(/<8
FA'2A<(%/&2(2#5'(A'5%C.4(: (5/@3C%(#.(75%.7C<%55(#.(/;%<'(&##3%"/'A#<(&/<(>%(5%%<(FA'2A<('2%(%S/@3C%
8%5&"A>%8(A<('2%(3"%IA#75(5%&'A#<4(?<(3/"'A&7C/"E(8%'%&'A#<(#.(/(&#@>A<%8(53##.A<;(/''/&P(2/5
>%&#@%(3#55A>C%(#<C9(87%('#(&##3%"/'A#<(#.(/;%<'5(: M=! -(/<8(?M : *(#.('2%(2#5'(6*(/<8(: M=! -(#.
'2%(2#5'(OE(A4%4(87%('#(/(&##3%"/'A#<(#.(5#.'F/"%(%<'A'A%5(5A'7/'%8(#<(8A..%"%<'(2#5'54(H<%(@#"%
%S/@3C%(#.('2%(<%&%55A'9(/<8(75%.7C<%55(#.('2%(&##3%"/'A#<(#.(5%&7"A'9(/;%<'5(A5(#3%"/'A#<(#.('2%
P<#FC%8;%=>/5%8(/;%<'(?M : -4(?'(A5(A<'%<8%8('#(&#CC%&'(A<.#"@/'A#<(/>#7'(5753A&A#75(>%2/IA#"(#.
75%"5(/'(@/<9(%<'"9(3#A<'5(#.('2%(</'AI%(2#5'(/<8(%S&2/<;%(A<.#"@/'A#<(FA'2(5A@AC/"(/;%<'5(#.('2%
#'2%"(2#5'5('#(@/P%(A<'%;"/C(8%&A5A#<(/>#7'(5'/'75(#.(&#<<%&'A#<54(?<('2%(8%I%C#3%8(&/5%(5'789('2A5
/;%<'(2/5(>%%<(3"#IA8%8(>9(/(&#@3/"/'AI%C9(3##"(P<#FC%8;%(>/5%('#(3C/9(/(5A;<A.A&/<'("#C%(A<
A<'"75A#<(8%'%&'A#<4(?<('2%(.7"'2%"(8%I%C#3@%<'(#.('2%(&/5%(5'789(/(5A;<A.A&/<'(/&&%<'(FACC(>%(@/8%
#<(%<"A&2@%<'(#.(A'5(P<#FC%8;%(>/5%(/<8(#<('2%(A<&"%/5A<;(#.(A'5("#C%(A<(8A5'"A>7'%8(/''/&P(8%'%&'A#<4

O2%(&/5%(5'789(F/5(A@3C%@%<'%8(/5(/<(/33CA&/'A#<(#.('2%(5#=&/CC%8(D7C'A=/;%<'(695'%@
M%I%C#3@%<'(bA'(ZD : 6Mb[E(8%I%C#3%8(>9(/7'2#"5(#.('2A5(3/3%"4(D : 6Mb(A5(/(5#.'F/"%('##C(.#"
5733#"'(#.('2%('%&2<#C#;9(#.(@7C'A=/;%<'(595'%@5(.#"@/C(53%&A.A&/'A#<(/<8(A@3C%@%<'/'A#<4(?'
&#<5A5'5(#.(/(<7@>%"(#.(;%<%"A&(3"#&%87"%5E(;%<%"A&(8/'/>/5%(5'"7&'7"%5(/<8(%8A'#"5(F2A&2(@/P%(A'
3#55A>C%('#(53%&A.9(&#@3#<%<'5(#.('2%(@7C'A=/;%<'(595'%@(#<(/(.#"@/C(53%&A.A&/'A#<(C/<;7/;%(/<8
.7"'2%"('#(;%<%"/'%(@7C'A=/;%<'(595'%@(/"&2A'%&'7"%E(A'5(&#@@7<A&/'A#<(&#@3#<%<'5E('#(&C#<%
P<#FC%8;%=>/5%8(/;%<'5(FA'2('2%(<%%8%8(.7<&'A#</CA'9E(%'&4(WA57/C(1ccE(d : W : -(/<8(eD`
5#.'F/"%(F%"%(75%8('#(8%I%C#3('2A5('##C(PA'4(_#'A&%('2/'(8%I%C#3@%<'(#.('2%(@#8%C(/<8('2%(#>$%&'=
#"A%<'%8(3"#$%&'(#.('2%(&/5%(5'789(F%"%('2%(@#5'('A@%(/<8(%..#"'(&#<57@A<;(3/"'(#.(F#"P(F2%"%/5(A'5
5#.'F/"%(A@3C%@%<'/'A#<(FA'2A<(D : 6Mb(8%@/<8%8(@7&2(C%55('A@%(/<8(%..#"'54
Y7"'2%"("%5%/"&2(FACC(&#<&%"<('#('2%(8%I%C#3@%<'(#.(/("A&2%"(?<37'(O"/..A&(D#8%CE(%<"A&2@%<'(#.
P<#FC%8;%(>/5%5(#.(3/"'A&7C/"(/;%<'5(/<8(@%&2/<A5@5(.#"(8%&A5A#<(@/PA<;4(M%I%C#3@%<'(#.(/
5#.'F/"%(.#"(#..=CA<%(/;%<'(C%/"<A<;('#(A@3"#I%(5%&7"A'9(595'%@(3%".#"@/<&%(/<8('#(@/P%(3#55A>C9
A'5(/8/3'/>ACA'9('#(<%F(PA<85(#.(/''/&P5(A5(3C/<<%8(/5(F%CC4

Chapter 2. Results of Research on Digital Image Steganography: Approach, Techniques, Implementation and Simulation

Abstract.

This Chapter outlines concisely the main steganography oriented results of the Project. These results are twofold. The first result is the development of a new approach to transparent embedding data into digital images. This approach is capable to provide a tradeoff between high rate of the embedded data and robustness to common and some intentional distortions, in particular, to JPEG compression. The developed technique makes use the properties of the singular value decomposition (SVD) of a digital image. According to these properties each singular value specifies the luminance of the SVD image layer, whereas the respective pair of singular vectors specifies image geometry. Therefore slight variations of singular values cannot influence visibly on the cover image quality. The idea of the proposed approach is to embed a bit of data through slight modifications of singular values of a small block of the segmented covers. The approach is robust because it supposes to embed extra data into low bands of covers in a distributed way. The size of small blocks is used as an attribute to achieve a tradeoff between the embedded data rate and robustness as required by the application. An advantage of the approach is that it is blind. Simulation has proved its robustness to JPEG compression up to 40%. The approach can be used both for hidden communication and watermarking.

The second result is the development of the format for compressed representation of digital images to be embedded into cover one. The idea of compression is based on using SVD of image color matrices. SVD makes it possible to represent an image as a partial sum of the most significant layers corresponding to the largest singular values. This idea is applied to each small block of the segmented image. The developed format is capable to provide compression up to 2 bit/pixel. Combined with the developed technique for hiding data in digital images, it makes possible robust embedding digital image into a cover one.

All theoretical results are validated using thorough simulation on the basis of the developed software.

The detailed description of the aforementioned results can be found in [IntRep#1], [IntRep#2] [IntRep#3] and [FinRep#1].

2.1. Introduction: Overview of the Results Presented in Previous Reports.

Transparent hiding data into digital images called "digital image steganography" (DIS) presents an effective way for secret communication, watermarking and other applications. Although DIS is a quite new field of research, development of the Internet digital media and practical needs stimulated recent rapid progress in this field. Steganography by itself aims to conceal the very existence of the fact of communication. Combined with an encryption, steganography provides a higher level of the communication secrecy.

Currently this field is a subject of the intensive research. A number of techniques for DIS and watermarking have been developed during the last five years. In the Interim Report #1 [IntRep#1] the thorough overview of the state-of-the-art in DIS and watermarking areas were given. In this overview the steganography problems were analyzed in many respects. In particular, there were analyzed the terminology, classification of the embedding schemes, application-oriented classification of the embedding tasks and the respective common and particular requirements to image-based embedding techniques, general classification and overview of the developed approaches for hiding information in images. Let us summarize in brief the main results of this phase of the research.

According to the commonly accepted classification, the proposed DIS techniques can be classified as follows:

- Techniques that utilize a spatial domain. To insert data into an image, they use a selected subset of the image pixels[1] using a bit-wise approach ([Bender *et al-9*], [Bruyndonckx *et al*-95], [Chen *et al*-99], [Machado], [Matsui *et al*-98], [Pitas *et al*-96], [Tanaka *et al*-90], [van Schydel *et al*-94], etc.).
- Transform-based techniques, that operate with images represented by a finite set of orthogonal or bi-orthogonal functions called "basis functions" ([Burget et al], [Kundur *et al*-97], [Piva et al-97], [Podilchuck *et a*l-97], [Smith *et al*-96], [Xia et al-97], [Zhu et al-95], etc.). Examples are Discrete Cosine Transform, and Wavelet transform.
- Fractal-based techniques that construct "fractal code" of an image in such a way that allows to encode both the cover and the hidden images ([Puate et al-]).

More information on this subject can be found in [Cox et al-97], [Johnson *et al*-98], [Johnson *et al*-00], [Katzenbeisser *et al*-00], [Petitcolas *et al*-99], and [Swanson *et al* 98].

The common opinion is that there is no particular superior technique. Each technique has each own merit and flaws and preferable application area.

[IntRep#1] describes detailed classification of general and particular requirements to DIS techniques. In general, the major requirements to any DIS technique are assuring invisibility of the hidden data, robustness to common and some types of intentional distortions and support a required rate of the hidden data. Since these requirements are conflicting, and concrete requirements are different for different application areas, the rational tradeoff depends on any particular application ([Petitcolas *et al*-98]).

Unfortunately, the majority of the techniques used for hiding data into digital images, known in the literature and implemented within commercial and research software tools are vulnerable to common signal processing and to intentional attacks involving distortions of sub-perceptual level. Many of the embedding systems provide a limited robustness against attacks. It was proved by employing software tools simulating such attacks, for example such tools as *StirMark, Unzign,* and *The Mosaic attack emulator.*

The lessons learnt by researchers on the basis of analysis of properties, advantages and disadvantages of the existing digital image steganography techniques are as follows [Petitcolas *et al*-98]:

1. Information hiding algorithms that attempt to meet all the accepted requirements to a steganography task solution would fail. There is no a superior solution applicable to all DIS tasks. Each solution must be based on a tradeoff depending on application, for example, robustness versus bandwidth and accessible rate of information to hide. It is quite definitely that the most real-life applications do not need to meet all requirements, to be *robust to all kinds of distortions* and to be *resistant against all* known and future types of *attacks*. For, possibly, every application one can find a technique that more or less meet the basic requirements, that more or less feasible.

2. Real problems are not only to insert and detect hidden data. According to [Petitcolas *et al*-98], the progress will come not just from devising new marking schemes, but in developing ways to recognize hidden data that have been embedded using obvious combinations of statistical and transform techniques and thereafter subjected to distortion.

3. It is common opinion that steganography would go through the same process of evolutionary development as cryptography, with an iterative process in which inventing new types of attacks will lead to the development of more robust systems [Petitcolas *et al*-98].

The above conclusions determined *the basic objectives of the steganography-oriented research of the Project.* Indeed, the study of the state-of-the-art in the DIS area exhibited that the majority of the developed techniques aims at solving the watermarking problem in which the most significant requirement is robustness to a wide range of distortions whereas high allowable rate of covertly embedded data is not an issue. That is why many existing approaches do not pay a noteworthy attention to the development of techniques capable to provide high rate of the invisibly embedded data and robustness, for example, to lossy compression like JPEG. Indeed, the only well-

[1] For example, using masking effect, or using a pseudo-random seeding or something other strategy.

known approach that could be used to embed an image into the cover one is embedding data into Least Significant Bit called as LSBs approach. One of such techniques was proposed in [Fridrich *et al*-99]. It uses segmentation of the image to be embedded into blocks of size *8×8*, applying DCT transform to each block, quantizing and encoding its coefficients and embedding each coded block into one or into two LSBs of the cover image. Unfortunately, such and similar techniques cannot provide robustness and are highly sensitive to many common distortions, image format transformations and JPEG compression.

However, many military and industrial applications, such as hidden communication (HC) and hidden transmission of digital images call for transparent and robust embedding of high volumes of data. Examples are transmission of top-secret projects, industry secret, plans of covert operations [Johnson *et al*-98], etc. An important aspect of HC is the necessity to support the survivability of the transmitted information.

Due to the theoretical limitations it is not possible to provide both high robustness and high rate of the transparently embedded data [Anderson *et al*-98]. Nevertheless, it is highly necessary to develop an approach that should be able to provide for the high rate of the transparently embedded data preserving a reasonable robustness.

Two ideas were chosen in the development of such an approach. The first of them is the development of a new robust method for embedding data into digital images and the second one is the development a format for compressed representation of the digital image to be embedded into cover one. Both these ideas were the subjects of the research during the second and sequential phases of the work.

This research resulted in the development of a new approach to the transparent embedding data into digital images, which was described in [FinRep#1], [Gorodetski3 *et al*-00] and [Gorodetski4 *et al*-00]). The developed approach can be classified as a "Transform-based" because it deals with the image transformed to the Singular Value Decomposition (SVD). The developed method uses the properties of SVD of a digital image. According to these properties, each singular value (SV) specifies the luminance (energy) of the SVD image layer, whereas the respective pair of singular vectors specifies the image geometry. Therefore, slight variations of SVs cannot affect the visual perception of the quality of the cover image. The proposed approach is based on the embedding of data through slight modifications of SVs of a small block of the segmented cover image. The approach is potentially robust because it embeds extra data into low bands of the cover image in a distributed way. The size of small blocks can be used as an attribute to achieve a tradeoff between the embedded data rate and robustness. An additional advantage of the approach is that it is blind, i.e. it allows extracting hidden information without using of the original cover image. Below in following sections the developed approach to embedding data into digital images is described in more details.

The second idea resulted in the development of the new format for the compressed representation of digital images. This format is implemented and explored in details via simulation ([IntRep#2], [Gorodetski3 *et al*-00], [Gorodetski4 *et al*-00]). The approach is based on using singular value decomposition (SVD) of every image color matrices. SVD makes it possible to represent an image as a partial sum of the most significant layers corresponding to the largest singular values. The idea of such compression is that contribution of each *i-th* layer into forming of the original image is proportional to λ_i, since singular vectors are normalized. That is why potentially it is possible to delete the layers corresponding to the small singular values without noticeable degradation of the resulting image as compared with the original one. Extended simulation confirmed that this guesswork is valid for preserving no more than 25% of the most significant layers

The aforementioned idea was used for the development of a new image compressed format for compressed image coding. It makes use of

(1) a number of the MSLs determined according to a simple formal criterion and validated through simulation,

(2) segmentation of the image into small blocks of a size depending on the required data bit rate to be embedded and required quality of the target image after decompression,

(3) special quantization and

(4) optimal encoding of singular vectors of the preserved MSLs.

Simulation proved that this format can provide less than *2 bpp* data rate while preserving needed quality of the restored image. Although the last result can be thought as in some sense aside as compared with the Project objectives, nevertheless, while combining with the developed SVD-based approach for hiding data in digital images, it allows to embed robustly a digital image into a cover one. To our knowledge, there are no other methods that are capable to embed a digital image into a cover one in a way that provide robustness to the JPEG compression.

The rest of the chapter is devoted to the description of the developed SVD-based method of hiding data into digital images. In Section 2.2 the concept of the proposed approach is explained. In Section 2.3 the developed techniques of data hiding are described and the results of a simulation-based study, focused on the robustness issue as well as on embedded data rate are outlined. The developed technique is illustrated by several examples. In conclusion a general assessment of the results is given.

2.2. Mathematical Basis of the Developed Techniques for Hiding Data into Digital Images: Singular Value Decomposition of Digital Images

A digital image in bitmap format is specified by a *m*×*n* matrix $A = \{a_{i,j}\}_{m,n}$. If an image is represented in RGB format then it is specified by three such matrices A_R, A_G and A_B.

An arbitrary matrix ***A*** of size *m*×*n* can be represented by its SVD ([Horn *et al*]) in the form

$$\boldsymbol{A} = \boldsymbol{X\Lambda Y}^T = \sum_{i=1}^{i=r} \lambda_i X_i Y_i^T \qquad \textbf{(1)}$$

where ***X, Y*** are orthogonal *m*×*m* and *n*×*n* matrices respectively, $X_1, X_2, ..., X_m$ and $Y_1, Y_2, ..., Y_n$ are their columns, ! is diagonal matrix with non-negative elements, and $r \le \min\{m, n\}$ is the rank of the matrix ***A***. Diagonal terms $\lambda_1, \lambda_2, ..., \lambda_r$ of matrix ! are called *singular values* (SV*)* of the matrix ***A*** and *r* is the total number of non-zero singular values. Columns of the matrices ***X, Y*** are called *left* and *right* singular vectors of the matrix ***A*** respectively. Singular values $\lambda_1, \lambda_2, ..., \lambda_r$ can be calculated as $\lambda_i = \sqrt{\mu_i}$ *i=1,2,…,r,* where μ_i is an eigenvalue of the matrix AA^T, or $A^T A$. The left singular vector X_i, $i = 1,2,...,r,$ is equal to the eigenvector of the matrix AA^T corresponding to μ_i. Similarly, the right singular vector Y_i, $i = 1,2,...,r,$ is equal to the eigenvector of the matrix $A^T A$ that corresponds to its eigenvalue μ_i. If an image is given in RGB format then it is represented by three SVDs in the form (1).

Thus, SVD of an image decomposes the respective matrix into layers $\lambda_1 X_1 Y_1^T$, $\lambda_2 X_2 Y_2^T$,…, $\lambda_s X_r Y_r^T$. As a rule, SVs are enumerated in descending mode, i.e. if $\lambda_i > \lambda_j$ then *i<j,* and λ_1 is the maximal SV.

SVD possesses several interesting properties ([Horn *et al*]; two of them are utilized below to achieve invisible and robust hiding of extra data in digital images.

The first property is that each SV specifies the luminance (energy) of the SVD image layer, whereas the respective pair of singular vectors specifies an image "geometry". It was discovered that slight variations of SVs do not affect visual perception of the quality of the cover image. This property is used to embed a bit of data through slight modifications of SVs of a small block of a segmented cover.

The second property is that without the loss of image quality an image could be represented by so-called Truncated SVD (TSVD), i.e. by the sum

$$A_s = \sum_{i=1}^{i=s} \lambda_i X_i Y_i^T \text{ , } s << r. \tag{2}$$

instead of sum (1) ([Gorodetski3 *et al*-00]). In other words, a TSVD of an image can be used for its compressed representation. SVD-based image compression was proposed in [Andrews *et al*-76]. Later a number of approaches that combine SVD image transform with other transforms was developed. However, the major attention was paid to the development of a *lossyless* SVD image compression and its combinations with other transforms. For example, to code images, in [Yang *et al*-95] SVD transform is combined with Vector Quantization approach, in [Waldemar *et al*-97] a combination of SVD and Karhunen-Loeve transform is used to develop a hybrid compression. In [Fukutomi *et al*-99] SVD transform is combined with wavelet transform. In [Gorodetski3 *et al*-00] a format for SVD-based *lossy compression* of digital images was proposed. This format provides the rate of compression close to 2 bit/pixel while preserving the appropriate quality of the restored image. This format is used to solve the task of robust embedding a digital image into a cover one.

2.3. SVD-based Techniques for Hiding Data into Digital Images

The following are the techniques that were developed to utilize the first of the two aforementioned properties of SVD image representation.

2.3.1. Technique 1

In brief, the first proposed technique is as follows. A cover image represented in 24 bpp (RGB) format is segmented into blocks of size s×s[1] and SVDs *for each such a block* and *for each matrix* of *Red, Green and Blue layers* are computed. Each block of every color layer is used to embed a bit of data. In the Technique 1, a bit of data is embedded through a slight modification of the largest singular value of the block. The implemented and explored algorithm of modification is described below.

Let *B(k,l)* be a block, where *k* is the block number and *l*∈*{Red, Green, Blue}.* Let the largest SV of the block *B(k,l)* of size s×s be λ_1^k . Let *b* be a bit of data to be embedded into this block. The embedding algorithm is as follows:

For each pair (k, l)

1. Choose the quantization step, *d*, of the largest singular value of the block. The value *d* may be different depending on the layer of color.[2]
2. Compute integer number *S* such that $\lambda_1^k (l) = S \times d + \delta$, $\delta < S$.
3. Embed bit *b* of data as follows:

```
If S is the odd number then
    if b=1 then S is not changed
  else
    if b=0 then S:=S+1.

If S is the even number then
  if b=1, then S:=S+1, else
    if b=0, then S is not changed.
```

[1] The developed software implements a particular case of this technique when *s=4*, generally, this number could be extended. Note that an increase of *k* value results in the increased robustness of the technique and in the decreased volume of transparently embedded data.

[2] The value of *d* is selected on the basis of statistical exploration of correlation between distortion caused by JREG compression of various percentages and the probability of a bit recovery. This exploration must be made for each color. The respective results are given below in this section.

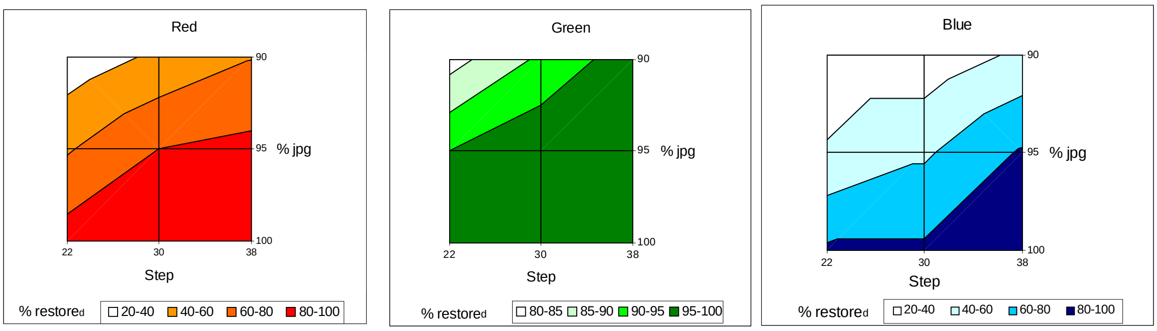


Fig. 2.1. The plots of dependencies between the step of quantization *d* of the largest singular value of a cover image and survivability of the embedded image after JPEG compression for *red* (left), *green* (center) and *blue* (right) color layers of the cover image. These results correspond to the case when cover image is segmented into blocks of size 4×4

4. Compute the modified singular value $\tilde{\lambda}_1^k(l)$:

$$\tilde{\lambda}_1^k(l)=d\times S+d/2.$$

5. Compute the matrix of the block having modified largest singular value:

$$\tilde{B}(k,l)=\tilde{\lambda}_1^k(l)X_1(l)Y_1^T(l)+\sum\nolimits_{i=2}^{4}\lambda_i(l)X_i(l)Y_i^T(l)$$

6. Result: Matrix $\tilde{B}(k,l)$ containing embedded bit of data.

The major implementation concern of the above algorithm is how to choose the quantization step *d*. It is obvious that the increase of the value *d* leads both to more robust data hiding and to less transparency of the embedded data. To explore this dependency quantitatively, the respective simulation was performed for several cover images segmented into blocks of size 4×4 pixels and several images to be embedded. The latter were segmented into small blocks of size 8×8 and then compressed using TSVD proposed in [Gorodetski3 *et al*-00] and mentioned in Section 2. The results are given in Fig.2.1a (for *Red* layer), Fig.2.1.b (for *Green* layer) and Fig.2.1.c (for *Blue* layer). The plots illustrate the correlation between the percentage of JPEG compression and percentage of the correctly recovered blocks of the embedded image. Based on this result the following values of quantization steps within the *Red*, *Green* and *Blue* layers were chosen:[1]

d(red)=46, d(green)=22 and *d(blue)=52*.

It should be noticed that the quantization step value *d* might be used as a component of the secret key providing the restricted access to the hidden information.

The simulation indicated that this way of embedding data into a cover image is robust against 100% JPEG compression.

The hidden data extraction procedure is very simple. Let $\tilde{B}(k,l)$ be a block with an embedded bit of data.

For each pair (k, l) do

1. Compute the largest singular value $\tilde{\lambda}_1^k(l)$.
2. Compute $\tilde{\lambda}_1^k(l)/d=S+d/2$.
3. If *S* is even number then the embedded bit value is *0* otherwise it is *1*.

[1] Note that the appropriate choice is specific for every way of cover images segmentation.

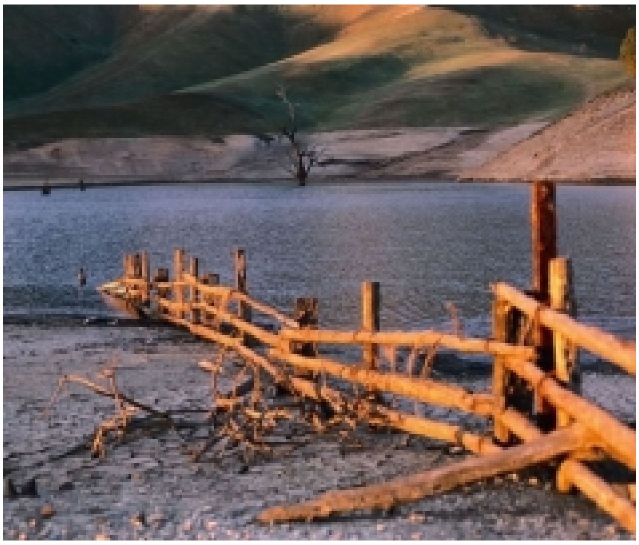


Fig.2.2.a. Cover image. It is presented in RGB format and is of size 600×512 pixels

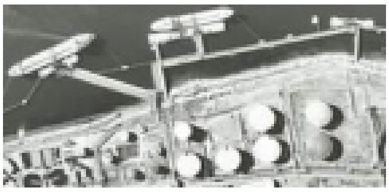


Fig.2.2.b. Image to be transmitted. It is gray and is of size 240×120

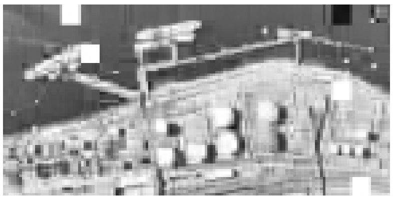


Fig.2.2.c. Recovered hidden image. The stego-image was subjected to JPEG compression

Fig. 2.2. An example of the use of the Technique 1 for embedding image into cover one

This approach to data embedding provides a sufficiently high rate of the embedded data although its bit rate is less than the one provided by LSBs techniques. For example, let cover image be of size 600×512 (see Fig.2.2.a) and $s=4$. It comprises 150×128 blocks of size 4×4 in each color. Therefore this technique makes it possible to embed up to 57600 bits. The picture to be embedded (see Fig.2.2.b) is of size 240×120 and segmented into 200 blocks of size 12×12. Due to TSVD compression (see Section 2.2), each such block is represented into blocks of 12×12 using segmentation. Its length is 288 bits, that is why the total size of the image of Fig.2b in TSVD format is equal to 56000 bits. Hence, it is possible to embed it into image depicted in Fig.2.2.a.

This technique was subjected to several experimental studies. An example of such a study is given in Fig.2.2. The cover image (Fig.2.2a) containing embedded image (Fig.2.2b) was distorted by JPEG compression and then transformed back in BMP format. The hidden image extracted from the JPEG distorted stego-image is depicted in Fig.2.2.c. One can see that the quality of the reconstructed image is not excellent but is very satisfactory. Notice that the bit rate of the TSVD image to be embedded can be increased using a Haffman-like compression of the TSVD files for each block.

Embedding and recovery procedures could be equipped with a secret key to seed blocks thus providing additional level of security. To improve the survivability of the hidden data during transmission it is possible to transmit the same image several times using various covers. It should be noticed that if the image to be hidden is of very large size then its transmission could be implemented using several cover images.

2.3.2. Technique 2

This technique uses a different approach to embed data into a cover image. Notice that the type of embedded binary file is irrelevant. A bit of information is embedded into a block of the segmented cover image. The block size could be chosen arbitrarily.

Let cover image be represented in a 24 bit (RGB) format. Data can be embedded independently into each RGB layer of the cover image or, optionally, in specified layer(s). Let the size of blocks of the cover image segmentation be $m \times k$ pixels, A be the matrix of a block of the covers corresponding to a color layer from *Red*, *Green* or *Blue*. Let a bit b to be embedded into block A of a layer.

The algorithm of the *embedding procedure* is as follows:

1. Compute singular value decomposition of matrix *A*. Let V^{λ}=[$\lambda_1, \lambda_2, ..., \lambda_r$] be the vector of singular values of matrix *A* ordered in decreasing mode, X_i and Y_i are singular vectors of matrix *A* and *i=1,2,…,r,* where *r* is the rank of matrix *A*.
2. Compute Euclidean norm of vector V^{λ}, *Norm*(V^{λ})=$\sqrt{\sum_{i=1}^{r}(v_i^{\lambda})^2}$, where v_i^{λ}, *i=1,2,…,r,* are the components of vector V^{λ}.
3. Select the value of *Delta* that is the step of quantization of the Euclidean norm of vector V^{λ}.

   Remark 1. The appropriate value of *Delta* depends on the color layer used for embedding a bit of data and has been chosen for each layer through simulation. Notice that the value of *Delta* can play the role of a component of *the secret key* restricting access to the hidden data. One more way to increase the secrcy is to use an uneven quantization of *Norm*(V^{λ}).

4. Compute the integer *N=[Norm(*V^{λ}*)/Delta]*, where [*] is the integer part of the quotient of division.
5. Embed bit *b* according to the following algorithm:

```
If $b=1$ then
{if $N$ is odd then $\tilde{N}=N+1$ else $\tilde{N}=N$}
else (if $b=0$)
{if $N$ is even then $\tilde{N}=N$ else $\tilde{N}=N+1$}}
```

6. Compute the modified norm of the vector of the singular values:

$$Norm(\tilde{V}^{\lambda})=\tilde{N}\times Delta+(Delta/2).$$

7. Compute the modified vector of the singular values:

$$\tilde{V}^{\lambda}=V^{\lambda}\times(Norm(\tilde{V}^{\lambda})/Norm(V^{\lambda})).$$

8. Compute the modified matrix of the block in which bit *b* is embedded:

$$\tilde{A}=\sum_{i=1}^{r}\tilde{\lambda}_i X_i Y_i^T.$$

9. End of the embedding procedure.

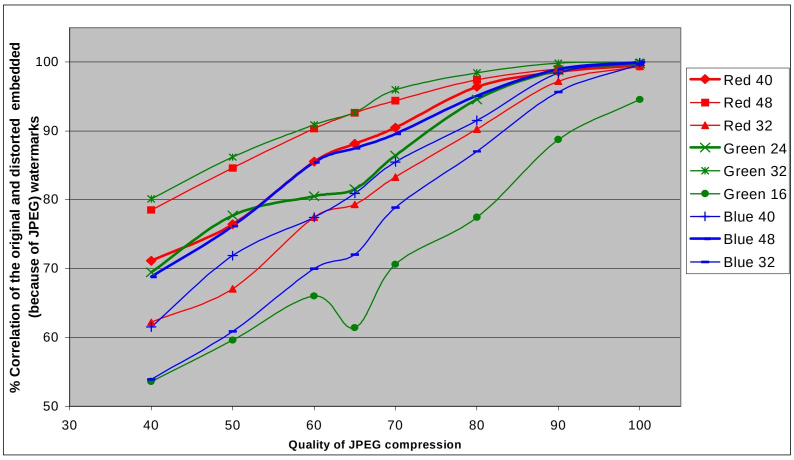


Fig. 2.3. Dependencies between degree of JPEG compression (horizontal) and probability of the watermark presence (vertical) for various value *Delta.* (Averaged over a set of images)

The described algorithms must be applied to each block of the covers in which a bit of data is to be embedded.

The embedding procedure may provide restricted access to the hidden data via using seeding of the binary string to be embedded in pseudo random mode or via transpositions of the lines and columns [Gorodetski3 *et al*-00].

The extraction task is simpler then the embedding. Let $\tilde{A}$ be the matrix of block containing hidden bit *b* of data, which must be extracted.

1. Compute the singular value decomposition of block $\tilde{A}$. Let $\tilde{V}^{\lambda}$ be vector of singular values ordered in decreasing fashion, X_i and Y_i are singular vectors of matrix $\tilde{A}$ and *i=1,2,…,r*, where *r* is the rank of matrix $\tilde{A}$.

   Remark 2. SVs and singular vectors of the same block $\tilde{A}$ of the modified cover image can be additionally modified during transmission or changed intentionally. For simplicity, we denote them in the same way as they were denoted in the embedding procedure.

2. Compute the Euclidean norm of vector $\tilde{V}^{\lambda}$, i.e. *Norm* $\tilde{V}^{\lambda} = \sqrt{\sum_{i=1}^{r}(\tilde{v}_i^{\lambda})^2}$.
3. Compute $\tilde{N}$ *=[Norm*$\tilde{V}^{\lambda}$ */Delta]*, where [*] is the integer part of the quotient of division.
4. Compute the value of the hidden bit *b*:

   {If $\tilde{N}$ *is even then b=1 else b=0}*

5. End of extraction procedure.

The described embedding (extraction) algorithm must be applied to each block of the covers (stego-image), in which a bit of data is embedded. The extracting procedure may require the knowledge of the secret key if it has been applied in embedding.

This technique was investigated statistically from several points of view. The first task was to explore the optimality of *Delta* values in the trade-off between the robustness of the hidden data and its visibility. It was established that the appropriate value of *Delta* depends on the color layer. In fig.3 the results of the simulation-based investigation of the aforementioned dependencies are given. One can see that optimal choices of the of Delta given color layer are close to the followings:

Delta(*Red*)=40, *Delta*(*Green*)=24, *Delta* (*Blue*)=48.

Given such values of *Delta*, Technique 2 proves robustness to JPEG compression up to degree 40% provided that the value of the watermark presence probability is (0.7–0.8).

The special attention was paid to study the relationship between the degree of JPEG,

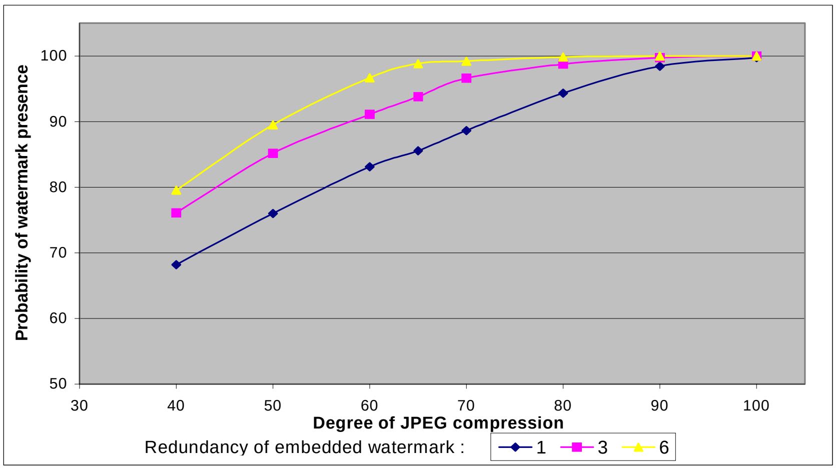


Fig. 2.4. Dependency between *Degree of JPEG compression* (horizontal axis) and *Probability of the watermark presence* for various degrees of redundancy

compression redundancy of the embedded watermark and the probability of the watermark presence. In this study redundancy is understood as the number of embedded copies of the watermark. The results are displayed in Fig.2.4. One can see that the redundancy presents an additional way to increase the robustness of Technique 2.

In fig.2.5 an example of using Technique 2 for embedding emf-file into a digital image is given. Left-hand image (fig.5a) corresponds to the cover image (in gray scale) with the embedded emf-file. The right-hand image depicts the cover image with extracted data that indicates, for example, to a pilot the route to follow that was hidden into transmitted image.

2.4. Conclusion of the Chapter 2

This Chapter presents the main final result of the steganography-oriented research on the Project. It is a novel approach to digital image steganography and two particular techniques implementing this approach. Both techniques utilize the concept of embedding data through slight modifications of singular values of small blocks of the cover image.

The techniques, implemented in software, are subjected to statistical analysis of their robustness and the allowable rate of covertly embedded data. In particular, it is shown the developed approach for data hiding is robust to JPEG compression up to 40%. It is blind, i.e. the hidden data can be extracted without possessing the original cover image. Embedding and recovery procedures can be equipped with a password and secret key to seed blocks thus providing restricted assesses to the hidden data. There exist several additional attributes resulting in additional security assurance.

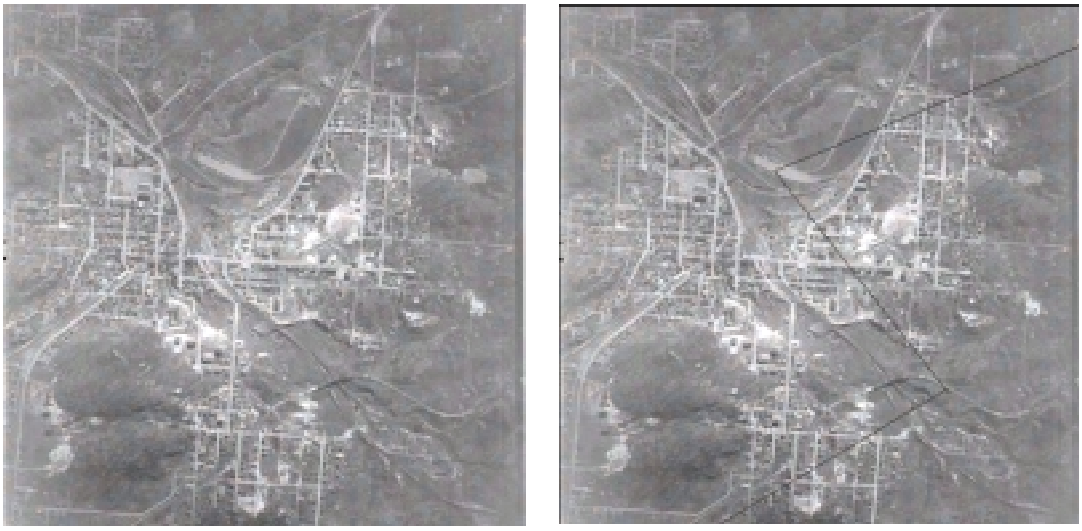


Fig.2.5.a. Cover image containing invisibly embedded *emf*-file representing an aircraft route

Fig.2.5.b. Extracted route drawn over the cover image

Fig. 2.5. An example of the use of the Technique 2 to hide route of an aircraft into the map. The hidden data are represented in *emf* graphical format.

The analyses indicate that the developed techniques are suitable for hidden communication that calls for high rate and appropriate survivability of the embedded data, and invisibility of the hidden image, and for watermarking where the main requirement is robustness to common and some intentional distortions.

The approach is demonstrated by several examples of practical applications.

3. General Conclusion on the Project

According to the Project Work Plan the main tasks that the Project was addressing to are as follows:

1) Development of the architecture of the agent-based information security system on the whole and architectures of particular agents; development of the ontology of information security domain to design and to decompose distributed knowledge base structure.
2) Development of a formal framework for representation of the agents' distributed knowledge.
3) Development of the procedure of the agents' cooperation for integrated information security task solving.
4) Development and mathematical justification of the new methods of image-based information hiding (image-based steganography) to provide safe channels of information exchange.

All aforementioned tasks were solved and the results were submitted to the Partner in three Interim and two Final reports. The results of the research were published in proceedings of seven international conferences and workshops with reviewed articles. Two papers have been accepted already to the forthcoming international workshop on computer network security.

This Report presents the final results of the research. The Project objectives include two in some sense independent tasks. One of them concerns to the multi-agent model and software prototype of the computer network security system and the other one concerns to the digital image steganography. Accordingly, this Final Report comprises two chapters. Each of them is devoted to the brief outline of the respective results submitted in previous reports and to the description of the new results that were achieved during the final phase of the research. In both Chapters we accentuate the software developed for verification and validation of the theoretical results, i.e. for verification and validation of the developed approaches, methods, architectures, techniques and algorithms associated with the Project tasks.

The Chapter 1 considers the developed Case Study of the network security system that is a software implementation of the multi-agent security system. The Case Study is composed of particular autonomous knowledge-based agents, distributed over the hosts of the computer network to be protected and cooperating to make integrated consistent decisions. The Chapter 1 describes the architecture of the security system Case Study and architectures of its components that are particular software agents, communication components and software that is intended to simulate the input traffic. The Case Study architecture corresponds to the multi-agent system protecting a segment of a Local Area Network comprising four hosts to be protected. Each host-based component of the network security system comprises seven specialized software agents situated on the host. In total, the Case Study comp[rises 28 distributed over the network interacting software agents.

Simulation of the Case Study displayed a number of advantages of multi-agent architecture for protection of a computer network against distributed attacks. The most significant of them is a capability of the comparatively "light" components of a multi-agent security system to cooperate to solve a "heavy" task. At present the only way to detect efficiently a distributed attack against a computer network is a cooperation of security software entities (agents) distributed over the hosts of the network and within each host itself. A sample of usefulness of agent cooperation can be seen within the described example. In particular, detection of a *combined spoofing attack* has become possible only due to cooperation of the software agents situated on different hosts. One more example of the necessity and usefulness of the cooperation of security agents is operation of the knowledge-based agent named IDA2. It is intended to collect information about suspicious behavior of users at many entry points of the native host and exchange information with similar agents of the other hosts to make integral decision about status of connections. In the developed case study this agent has been provided by a comparatively poor knowledge base and can not play a significant role in intrusion detection. In the further development of the case study a significant accent must be made on enrichment of its knowledge base and on the increasing its role in distributed attack detection.

This Case Study is implemented as distributed multi-agent system, which components interact via message exchange. Simulation scenario, input traffic model and peculiarities of the distributed security system operation are described. The major attention is paid to the intrusion detection task and agents' interactions during detection of an attack against the computer network. Case Study implementation was carried out on the basis of the Multi-agent System Development Kit developed by authors of the research.. The software code is developed using Visual C++, JAVA 2 and XML.

The Chapter 2 outlines concisely the main steganography oriented results of the Project. These results are twofold. The first result is the development of a new approach to transparent embedding data into digital images. This approach is capable to provide a tradeoff between high rate of the embedded data and robustness to common and some intentional distortions, in particular, to JPEG compression. The developed technique makes use the properties of the singular value decomposition (SVD) of a digital image. According to these properties each singular value specifies the luminance of the SVD image layer, whereas the respective pair of singular vectors specifies image geometry. Therefore slight variations of singular values cannot influence visibly on the cover image quality. The idea of the proposed approach is to embed a bit of data through slight modifications of singular values of a small block of the segmented covers. The approach is robust because it supposes to embed extra data into low bands of covers in a distributed way. The size of small blocks is used as an attribute to achieve a tradeoff between the embedded data rate and robustness as required by the application. An advantage of the approach is that it is blind. Simulation has proved its robustness to JPEG compression up to 40%. The approach can be used both for hidden communication and watermarking.

The second result is the development of the format for compressed representation of digital images to be embedded into cover one. The idea of compression is based on using SVD of image color matrices. SVD makes it possible to represent an image as a partial sum of the most significant layers corresponding to the largest singular values. This idea is applied to each small block of the segmented image. The developed format is capable to provide compression up to 2 bit/pixel. Combined with the developed technique for hiding data in digital images, it makes possible robust embedding digital image into a cover one.

All theoretical results of the Project are validated using thorough simulation on the basis of the developed software. The developed software will be demonstrated and submitted to the Partner.

References

[Allen *et al*-00] J.Allen, A.Christie, W.Fithen, J.McHugh, J.Pickel, E.Stoner. State of the Practice of Intrusion Detection Technologies. In: Technical Report CMU/SEI-99-TR-028, Carnegie Mellon Software Engineering Institute, January 2000, 220 pp.

[Anderson *et al*-95] D Anderson, T Frivold, and A Valdes. Next-generation intrusion-detection expert system (NIDES). Technical Report SRI-CSL-95-07, Computer Science Laboratory, SRI International, Menlo Park, CA, USA, May 1995.

[Anderson *et al*-98] R.Anderson, F.A.P.Petitcolas. On the Limits of Steganography. *IEEE Journal of Selected Areas of Communications.* 16(4), pp.474-481, 1998.

[Andrews *et al*-76] H.C.Andrews, C.L.Patterson. Singular Value Decomposition (SVD) for Image Coding. *IEEE Transaction on Communication*. Vol. 24, 1976, pp.425-432.

[Asaka *et al*-99] M.Asaka, S.Okazawa, A.Taguchi, S.Goto. A Method of Tracing Intruders by Use of Mobile Agents. In: *Proceedings of INET'99*, June 1999.

[Axelsson-00] S.Axelsson. Intrusion Detection Systems: A Survey and Taxonomy. In Technical Report No 99-15, Dept. of Computer Engineering, Chalmers University of Technology, Sweden, March 2000.

[Bace-99] R.Bace. An Introduction to Intrusion Detection & ASSESSMENT for System and Network Security Management. Infidel, Inc. 1999.

[Balasubramaniyan *et al*-98] J.S.Balasubramaniyan, J.O.Garcia-Fernandez, D.Isacoff, E.Spafford, D.Zamboni. An Architecture for Intrusion Detection Using Autonomous Agents. Coast TR 98-05. West Lafayette, In: COAST Laboratory, Purdue University, 1998.

[Bender *et al-96*] W.Bender, D.Gruhl, N.Morimoto, and A.Lu. Techniques for Data Hiding. In: *IBM System Journal*, 35(3&4), 1996.

[Bonifácio *et al*-98] Jr.Bonifácio, A.Cansian,, E.Moreira, and A.de Carvalho. An Adaptive Intrusion Detection System Using Neural Networks. *Proceedings of the IFIP World Computer Congress–Security in Information Systems, IFIP-SEC'98*, Chapman & Hall, Vienna, Austria (1998)

[Bradshaw-97] J.M.Bradshaw. An introduction to software agents. In: *Software Agents*, AAAI Press/The MIT Press, 1997.

[Bruyndonckx *et al*-95] O.Bruyndonckx, J.J.Quisquater, and B.Macq. Spatial Method for Copyright Labeling of Digital Images. In: *Proceedings of IEEE Workshop on nonlinear signal and image Processing*, Greece, 1995.

[Burget *et al*-94] S.Burget, E.Koch, and J.Zhao. A Novel Method for Copyright Labeling Digitized Image Data. Technical Report, Fraunhofer Institute for Computer Graphics, Germany, 1994.

[Chen *et al*-99] B.Chen and G.W.Wornell. Dither Modulation: A new Approach to Digital Watermarking and Information Embedding. In: Ping Wah Wong and E.J.Delp (Eds). Vol. 3657, San Jose, CA, USA, January 1999.

[Conner *et al*-99] M.Conner, C.Patel, M.Little. Genetic Algorithm/Artificial Life Evolution of Security Vulnerability Agents. In: *Proceedings of 3rd Annual Symposium on Advanced Telecommunications & Information Distribution Research Program* (ATIRP). Army Research Laboratory Federal Laboratory. February 1999.

[Cox et al-97] I.J.Cox and M.Miller. A Review on Watermarking and the Importance of Perceptual Modeling. In: *Proceedings of the Conference on Electronic Imaging*, 1997.

[Crosbie *et al*-95] M.Crosbie, G.Spafford. Applying Genetic Programming to Intrusion Detection. In: *Proceedings of the AAAI Fall Symposium on Genetic Programming*. Cambridge, Menlo Park, CA, AAAI Press, 1995.

[Dasgupta-99] D.Dasgupta. Immunity-Based Intrusion Detection System: A General Framework. In: *Proceedings of the 22nd National Information Systems Security Conference* (NISSC), October, 1999.

[FinRep#1] Agent-Based Model of Information Security System: Architecture and Formal Framework for Coordinated Intelligent Agents Behavior Specification. Final Report #1, December 2000.

[IntRep#1] Agent-Based Model of Information Security System: Architecture and Formal Framework for Coordinated Intelligent Agents Behavior Specification. Interim Report #1, February 2000.

[IntRep#2] Agent-Based Model of Information Security System: Architecture and Formal Framework for Coordinated Intelligent Agents Behavior Specification. Interim Report #2 May 2000.

[IntRep#3] Agent-Based Model of Information Security System: Architecture and Formal Framework for Coordinated Intelligent Agents Behavior Specification. Interim Report #3, August 2000.

[Forrest *et al*-97] S.Forrest, S.Hofmeyr, A.Somayaji. Computer Immunology. In: *Communications of the ACM*, 40 (**10**), 1997, pp.86-96.

[Fridrich *et al*-99] J.Fridrich, M.Goljan. Protection of Digital Images using self-embedding. In: *Proceedings of the Second International Scientific Conference in the Republic of Kaazakhstan "Information Technologies and Control"*. Almaty, Kazakhstan, pp.302-311, 1999.

[Fukutomi *et al*-99] T.Fukutomi, O.Tahara, N.Okamoto, T.Minami. Encoding of Still Pictures by a Wavelet Transform and Singular Value Decomposition. In: *Proceedings of the 1999 IEEE Canadian Conference on Electrical and Computer Engineering.* Alberta, May 1999, pp.18-23.

[Goldberg *et al*-96] I.Goldberg, D.Wagner, R.Thomans, and E.Brewer. A secure environment for untrusted helper applications (confining the wily hacker). In: *Proceedings of the Sixth USENIX UNIX Security Symposium*, San Jose, California, USA, July 1996. USENIX, USENIX Association.

[Gorodetski1 *et al*-00] V.Gorodetski, I.Kotenko, L.Popyack, V.Skormin. Integrated Multi-Agent Information Security System: Mechanisms of Agents' Operation and Learning. In: *Proceedings of PAAM' 2000*. Manchester. UK. Practical Application Company Ltd. 2000. pp.151-154.

[Gorodetski2 *et al*-00] V.Gorodetski, I.Kotenko, V.Skormin. Integrated Multi-Agent Approach to Network Security Assurance: Models of Agents' Community. In: *Information Security for Global Information Infrastructures*. IFIP TC11 Sixteenth Annual Working Conference on Information Security (Eds. S.Qing, J.H.P.Eloff). Beijing. China. 2000, pp.291-300.

[Gorodetski3 *et al*-00] V. Gorodetski, V. Skormin, L.Popyack. Singular Value Decomposition Approach to Digital Image Lossy Compression. In*: Proceedings of the 4-th World Conference "Systems, Cybernetics and Informatics-2000" (SCI-2000*), Orlando, USA, July 2000.

[Gorodetski4 *et al*-00] V. Gorodetski, V. Skormin, L.Popyack. A Technique for Self-embedding of Digital Images. In: *Proceedings of Sixth International Workshop on Multimedia Information Systems (MIS2000)*. October 26-28, 2000, Marriott Chicago O'Hare, Chicago, USA.

[Habra *et al*-92] Jani Habra, Baudouin Le Charlier, Abdelaziz Mounji, and Isabelle Mathieu. ASAX: Software architecture and rule-based language for universal audit trail analysis. In: *Yves Deswarte et al., (eds), Computer Security*, Lecture Notes in Computer Science, Vol. 648, Springer-Verlag, 1992, pp. 435–450.

[Helmer *et al*-98] G.Helmer, J.Wong, V.Honavar, L.Miller. Intelligent Agents for Intrusion Detection. In: *Proceedings of the 1998 IEEE Information Technology Conference, Environment for the Future*. Syracuse. NY: IEEE, 1998. pp.121-124.

[Horn et al] R.A.Horn, C.R.Johnson. Matrix Analysis. Cambridge University Press, 1988.

[Ilgun-93] K.Ilgun. USTAT: A real-time intrusion detection system for UNIX. In: *Proceedings of the 1993 IEEE Symposium on Security and Privacy*, California, May 1993, IEEE Computer Press, pp.16– 28.

[Jackson *et al*-91] Kathleen A Jackson, David H DuBois, and Cathy A Stallings. An expert system application for network intrusion detection. In: *Proceedings of the 14th National Computer Security Conference*, Washington, D.C, October 1991, pp.215– 225, National Institute of Standards and Technology/National Computer Security Center.

[Jacobs *et al*-99] S.Jacobs, D. Dumas, W. Booth, M. Little. Security Architecture for Intelligent Agent Based Vulnerability Analysis. In: *Proceedings of 3rd Annual Symposium on Advanced Telecommunications & Information Distribution Research Program* (ATIRP). Army Research Laboratory Federal Laboratory. February 1999. pp.447-451.

[Jansen *et al*-00] W.Jansen, P.Mell, T. Karygiannis, D.Marks. Mobile Agents in Intrusion Detection and Response. In: *Proceedings of the 12th Annual Canadian Information Technology Security Symposium,* Ottawa, Canada, June 2000.

[Johnson *et al*-98] N.Johnson, S.Jagodia. Exploring Steganography: Seeing the Unseen. Computer, February 1998, pp.26-34.

[Johnson *et al*-00] N.Johnson, Z.Duric, S.Jajodia. Information Hiding. Steganography and Watermarking– Attacks and Countermeasures. Kluwer Academic Pub Books, 2000.

[Jou *et al*-97] Y.Jou, F.Gong, C.Sargor, S.F.Wu, and C.W Rance. Architecture design of a scalable intrusion detection system for the emerging network infrastructure. Technical Report CDRL A005, Dept. of Computer Science, North Carolina State University, Releigh, N.C, USA, April 1997.

[Karjoth *et al*-97] G.Karjoth, D.Lange, M.Oshima. A Security Model for Aglets. In: *IEEE Internet Computing*, August 1997. pp.68-77.

[Katzenbeisser et al-00] S.Katzenbeisser, F.A.P.Petitcolas (Eds). Information Hiding Techniques for Staganography and Digital Watermarking. Artech House Books. 220 pp., 2000.

[Kumar *et al*-94] S.Kumar and E.H. Spafford. A pattern matching model for misuse intrusion detection. In Proceedings of the 17th National Computer Security Conference, pp. 11– 21, Baltimore MD, USA, 1994. NIST, National Institute of Standards and Technology/National Computer Security Center.

[Kundur *et al*-97] D.Kundur, D. Hatzinakos. A Robust Digital Watermarking Method using Wavelet-based Fusion. In: *Proceedings of the International Conference on Image Processing*, Vol.1, USA, IEEE, 1997.

[Lee *et al*-99] W.Lee, S.J. Stolfo, K.Mok. A Data mining Framework for Building Intrusion Detection Model. In: *Proceedings of the IEEE Symposium on Security and Privacy* , 1999.

[Lindqvist *et al*-99] Ulf Lindqvist and Porras Phillip. Detecting computer and network misuse through the production-based expert system toolset (P-BEST). In: *1999 IEEE Symposium on Security and Privacy*, pp.146– 161, 1999.

[Lippmann *et al*-98] R.P.Lippmann, I.Graf, S.L.Garfinkel, A.S.Gorton, K.R.Kendall, D.J.McClung, D.J.Weber, S.E.Webster, D.Wyschogrod, and M.A.Zissman. The 1998 DARPA/AFRL off-line intrusion detection evaluation. Presented to The First Intl. Workshop on Recent Advances in Intrusion Detection (RAID-98), Lovain-la-Neuve, Belgium, September 1998.

[Lunt *et al*-88] T. F. Lunt, R.Jagannathan, R. Lee, S.Listgarten, D.L.Edwards, P.G. Neumann, H.S.Javitz, and A. Valdes. IDES: The enhanced proto-type, A real-time intrusion detection system. Technical Report SRI Project 4185-010, SRI-CSL-88-12, CSL SRI International, Computer Science Laboratory, SRI Intl., CA, USA, October 1988.

[Machado] R.Machado. EZ Stego. Http://www.stego.com.

[Matsui et al-98] K.Matsui and K.Tanaka. Video Steganography: How to Embed a Signature in a Picture. In: *Proceedings of IMA Intellectual property*, Vol. 1 (**1**), pp.187-206.

[Northcutt-99] S.Northcutt. Network Intrusion Detection: An Analyst's Handbook, New Riders, 1999.

[Paxon-98] V.Paxon. Bro: A system for detecting network intruders in real-time. In: *Proceedings of the 7th USENIX Security Symposium*, San Antonio, TX, USA, January 1988. USENIX, USENIX Association.

[Petitcolas *et al*-99] F.B.Petitcolas, R.J.Anderson, and M.Kuhn. Information Hiding–A Survey. In: *Proceedings of the IEEE, Special Issue on Protection of Multimedia Content.* 87(**7**), pp.1062-1078, 1999.

[Pitas et al-96] I.Pitas. A method for signature casting on digital images. In: *Proceedings of the International Conference on Image Processing (ICIP'96)*, 1996.

[Piva et al-97] A.Piva, M.Barni, E.Bartoloni, and V.Cappellini. DCT based Watermarking Recovering without Restoring to the uncorrupted original image. In: *Proceedings of the International Conference on Image Processing (ICIP)*, Vol.1, CA, USA, IEEE, 1997.

[Podilchuck *et a*l-97] C.I.Podilchuck, W.Zeng. Perceptual Watermarking of Still Images. In: *Proceedings of the Workshop on Multimedia Signal Processing*, Princeton, NJ, USA, 1997.

[Porras *et al*-97] P.A Porras and P.G Neumann. EMERALD: Event monitoring enabling responses to anomalous live disturbances. In: *Proceedings of the 20th National Information Systems Security Conference*, pp.353– 365, Baltimore, Maryland, USA, October 1997. NIST, National Institute of Standards and Technology/National Computer Security Center.

[Puate et al-96] J.Puate and F.Jordan. Using Fractal Compression Scheme to Embed a Digital Signature into an Image. In: *Proceedings of SPIE, Video Techniques and Software for Full-Service Network*, Vol. 2915, pp. 108-118, Boston, MA, USA, 1996.

[Ptacek *et al*-98] T.H.Ptacek, T.N.Newsham. Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection. Secure Networks, Inc. January, 1998.

[Queiroz *et al*-99] J.Queiroz, L.Carmo, L.Pirmez. Micæl: An Autonomous Mobile Agent System to Protect New Generation Networked Applications. In: *Proceedings of Second International Workshop on the Recent Advances in Intrusion Detection* (RAID'99). West Lafayette, Indiana, USA. 1999.

[Sebring *et al*-88] M.M. Sebring, E.Shellhouse, M.E. Hanna, and R.Whitehurst. Expert systems in intrusion detection: A case study. In: *Proceedings of the 11th National Computer Security Conference*, , Baltimore, Maryland, October 1988, pp.74– 81, NIST.

[Smaha-88] S. E. Smaha. Haystack: An intrusion detection system. In: *Proceedings of the IEEE Fourth Aerospace Computer Security Applications Conference*, December 1988. IEEE Computer Press, Los Alamitos, CA, USA.

[Smith *et al*-96] J.R.Smith and B.O.Comiskey. Modulation and Information Hiding in Images. In: *Lecture Notes in Computer Science*; Vol.1174, pp.207-226, Springer Verlag, 1996.

[Snapp *et al*-92] Steven R Snapp, Stephen E Smaha, Daniel M Teal, and Tim Grance. The DIDS (distributed intrusion detection system) prototype. In: *Proceedings of the Summer USENIX Conference*, pp. 227–233, Texas, June 1992. USENIX Association.

[Somayaji *et al*-98] A.Somayaji, S.Hofmeyr, S.Forrest. Principles of a Computer Immune System. In: *Proceedings of the 1997 New Security Paradigms Workshop*, 1998, pp..75-82.

[Staniford Chen-96] S. Staniford Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K Levitt, C. Wee, R. Yip, and D. Zerkle. GrIDS— A graph based intrusion detection system for large networks. In: *Proceedings of the 19th National Information Systems Security Conference*, 1996.

[Swanson *et al* 98] M.D.Swanson, M.Kobayashi, and A.H.Tewfic. Multimedia Data Embedding and Watermarking Technologies. In: *Proceedings of the IEEE*, 86(**6**), 1998, pp.1064-1087.

[Tanaka *et al*-90] K.Tanaka, Y.Nakamura, and K Mitsui. Embedding the Attribute Information into a Dithered Image. *Systems and Computers in Japan*, 21(**7**), 1990.

[van Schydel *et al*-94] R. Van Schydel, A.Tirkel, and C. Osborne. A digital Watermarking. In: *Proceedings of ICASSP*. Piscataway, NJ, IEEE press, 1994, Vol.II, pp.86-90.

[Vigna *et al*-98] G.Vigna, R.A.Kemmerer. NetSTAT: A Network-based Intrusion Detection Approach. In: *Proceedings of 14th Annual Computer Security Applications Conference*. Scottsdale, 1998.

[Waldemar *et al*-97] P.Waldemar, T.Ramstad. Hibrid KLT-SVD Image Compression. *Proceedings IEEE International Conference on Acoustics, Speech, and Signal Processing*. Germany, 1997, IEEE Computer Society Press, Vol.4, pp.2713-2716.

[White *et al*-96] G.White, E.Fisch, U.Pooch. Cooperating Security Managers: A Peer-Based Intrusion Detection System. In: *IEEE Network*, 10(**1**), 1996, pp.20-23.

[Xia *et al*-97]X.G.Xia, C.G.Boncelet, and G.R.Arce. A Multi-resolution Watermark for Digital Images. In: *Proceedings of International Conference on Image Processing (ICIP)*, Vol.1, USA, IEEE, 1997

[Yang *et al*-95] J-F.Yang, C-L.Lu. Combined Techniques of Singular Value Decomposition and Vector Quantization for Image Coding. In: *IEEE Transaction on Image Processing*, Vol. 4,(**8**), 1995, pp.1141-1146.

[Yang 00 *et al*-00] J.Yang, P.Ning, X.S.Wang, S.Jajodia. CARDS: A distributed System for Detecting Coordinated Attacks. In: *Information Security for Global Information Infrastructures. IFIP TC11 Sixteenth Annual Working Conference on Information Security* (Eds. by S.Qing, J.H.P.Eloff), Beijing. China. 2000.

[Zhu *et al*-95] B.Zhu, A.H.Tewfic, and O.Gerec. Low Bit Rate Near Transparent Image Coding. In: *Proceedings of International Conference on Wavelet Applications for Dual Use*, Vol. 2491, (Orlando, FL), pp.173-184, 1995.

Appendix A1. Case Study Model

A1.1. Structure of the basic concepts of the case study

One of the main concepts of the case study is the concept of “current connection”. This concept is for formation in CNSS of the generalized representation of the input messages (packets) sequence of one connection, and also for reflection of a current status of connection on the basis of processing of the messages, which has arrived to a current moment. This concept is a base for determination of the CNSS performance scheme. The CNSS performance process can be represented as the distributed processing of examples of this concept by various classes of the security agents according to their specialization.

When the first message, intended for a new connection activating, arrives on a host the agent AD-E of this host forms the description of the connection as an example of this concept. The attribute values of this example can vary dynamically as a result of the subsequent messages processing within the current connection. As the process of connections processing in a multiagent system is distributed, the different agents can have information on the same connection simultaneously. This information processing is coordinated according to the set scheme of agents’ interaction. At connection completion an appropriate example of concept “the current connection” is transferred in the completed connections archive.

The list of attributes used in the model of concept “current connection”, which is operated with the security agents of a host, is presented in the table A.1.

Table A.1.
The list of attributes used in model of concept “current connection”

ID	Unique identifier of an example of the concept “current connection”
IP address	IP-address of a host establishing the connection
Port destination	Number of a port, with which the connection is installed
Flag	Connection status
Last sqn_no	Sequence number of the last obtained tcp-packet
Access	Access rights
Time on	Time of the connection beginning
Time last tcp	Time of arrival of the last message obtained in connection
Time life	Life time of the connection in a “current status”
Fact	Fact of suspicious action, detected in connection
Data	Contents of a field “Data” of the last tcp-packet obtained in connection
N	Reserve numerical field

The value of a field *ID* is an unambiguous identifier of the example of concept “current connection”.

The values of attributes *IP address*, *Port destination* and *Time on* are assigned on the basis of parameters of the first *tcp*-message in connection and do not vary.

The field *Flag* identifies a current status of the connection. The list of possible statuses of the connection is defined on the scheme of transitions of the current connection statuses (Fig.A.1). *The main states of the connection* are the following:

- *HOC (Half Open Connection)* - status originating after the first phase of “hand shake”,
- *Set connection* - status originating after the third phase of “hand shake”,
- *Login* - status originating after identification and authentication of the user,
- *Closed* - completed connection (a transition in this status is carried out after generation of the TCP-message with a flag Fin or on time).

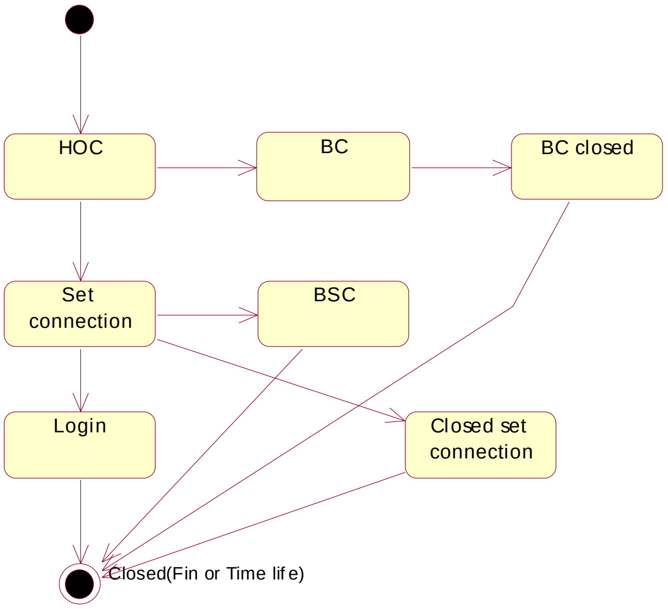


Fig.A.1. Scheme of transitions of the current connection statuses

The variation of the enumerated statuses of the connection happens as a result of arrival of the new messages.

Besides the statuses of the connection can vary automatically after defined time intervals. Thus the following classes of the connection statuses are selected:

- *BC (Bad connection)* - the status, in which the connection transfers from a status *HOC* after a time interval *Ack_wait_time*,
- *BC closed* - the status, in which the connection transfers from a status *BC* after a time interval *Bad_connection_life*,
- *BSC (Bad set connection)* - the status, in which the connection transfers from a status *Set connection* after a time interval *Set_connection_life*.

The time intervals of the connection existence under absence of the new messages are determined by means of values of attribute *Time life*. The instant defined by attribute *Time of last tcp* is used for time intervals counting. Besides the enumerated classes of the connection statuses defined as a result of the messages obtaining or on time, one more intermediate status causing suspicions is identified:

- *Closed set connection* - status originating after obtaining of the message with a flag Fin, when the connection is in a status *Set connection*.

The value of attribute *Last sqn_no* is updated at arrival of the new message. This attribute value is a formal tag for determination of the following message in connection.

The value of attribute *Access* sets within the connection access rights, which are determined during identification and authentication of the user.

If during the connection an action suspicious from a security view point is found out, this fact is fixed with usage of the attribute *Fact* value. If in the connection some facts of suspicious actions were detected, then a name of the last detected action class corresponds to this attribute. Thus there is no “loss” of the facts detected earlier, as the connections with the detected separate suspicious facts are recorded in the database of the agent *IDA2*. Thus, if during the connection some facts of suspicious actions are detected, all of them are recorded in the agent *IDA2* database.

In a field *Data* the data string from the same field of the last obtained message is stored.

Thus, the concept “current connection” is a basic concept for organization of the agents’ interaction in CNSS and for generation of the contents of the transmitted messages. On the basis of this concept the number of additional concepts for detection of the attack classes “Denial of service” and “port scanning” is implemented. The agents *AD-P1* use these concepts, therefore the determination of the concepts is considered at the description of the scripts of this class agent behavior.

A1.2. Scripts of the agents’ behavior

In this subsection the behavior scripts of the following agents’ classes is determined:

- *AD-E* – agents - demons of preprocessing of the input *tcp*-messages,
- *AD-P1* - agents - demons of pattern detection in connection till the moment of the users’ authentication and identification,
- *AD-P2* - agents - demons of pattern detection in connection after the moment of the users’ authentication and identification,
- *AIA* - identification and authentication agents,
- *ACA* - access control agents,
- *IDA1* – intrusion detection agents revealing a combined spoofing attack class,
- *IDA2* - intrusion detection agents revealing the complex attacks scripts.

The description of the all classes agents’ behavior is fulfilled under the following scheme.

At first a diagram is represented which determines (1) agents’ classes with which the agent of the circumscribed class cooperate, (2) content of the input and output messages as concept classes, (3) enumeration of the agents’ behavior scripts defined by the meta-rules. If for the agents’ class the more than one behavior script is determined, then a common meta-script of the agent’s behavior is also defined. This meta-script is responsible for choice of the necessary agent’s behavior script depending on the class and content of the input message.

Then a more detailed description of each behavior script is defined. The input of the scripts is fulfilled by means of the special editor that is a MASDK component. The user interface of this editor consists of several windows. The main window of the editor maps a general behavior script as a decision tree. The auxiliary windows map a detailed representation of separate rules of a decision tree. Further in the appendix text a common definition of the agents’ behavior scripts is given.

The Fig.A.2 (where MR – meta-rule) allows to restore a correspondence between the earlier circumscribed general representation of the behavior scripts (subsection 1.4) and that representation which is used in the main window of the editor.

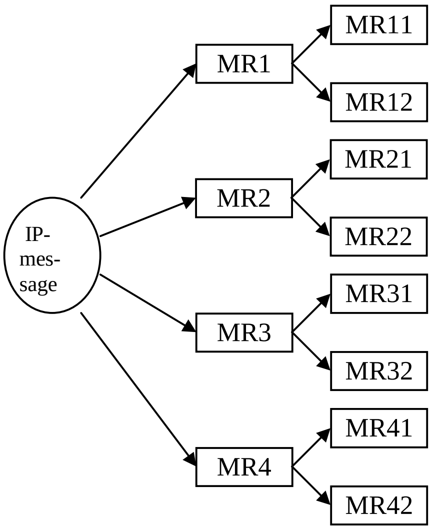


Fig.A.2. The representation of the agent *AD-E* behavior script (Script “A”)

A1.2.1. Scripts of the agent *AD-E* operation

The main task of an *agent-demon* is the preprocessing of the input tcp-messages arriving from *Input Traffic Model* (Fig.A.3). The preprocessing of such messages is fulfilled using data about the current connection, to which the input message concerns. Besides this messages the marks of model time and the facts concerning to current connections in a format of the current connection description can arrive on an input of the agent. The agent’s behavior script is selected depending on the contents of the arrived message on the basis of preset behavior model: the script *A* is selected for processing the tcp-messages, the script *B* - for processing the time stamps *time*, the script *C* - for processing the facts concerning to current connections.

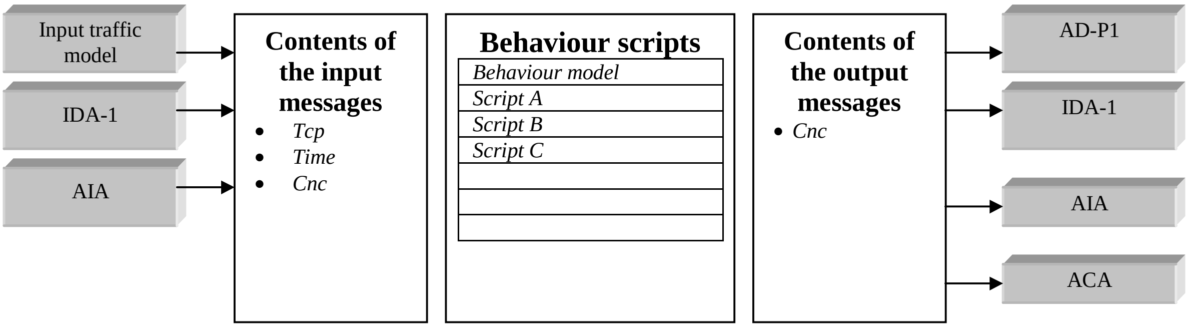
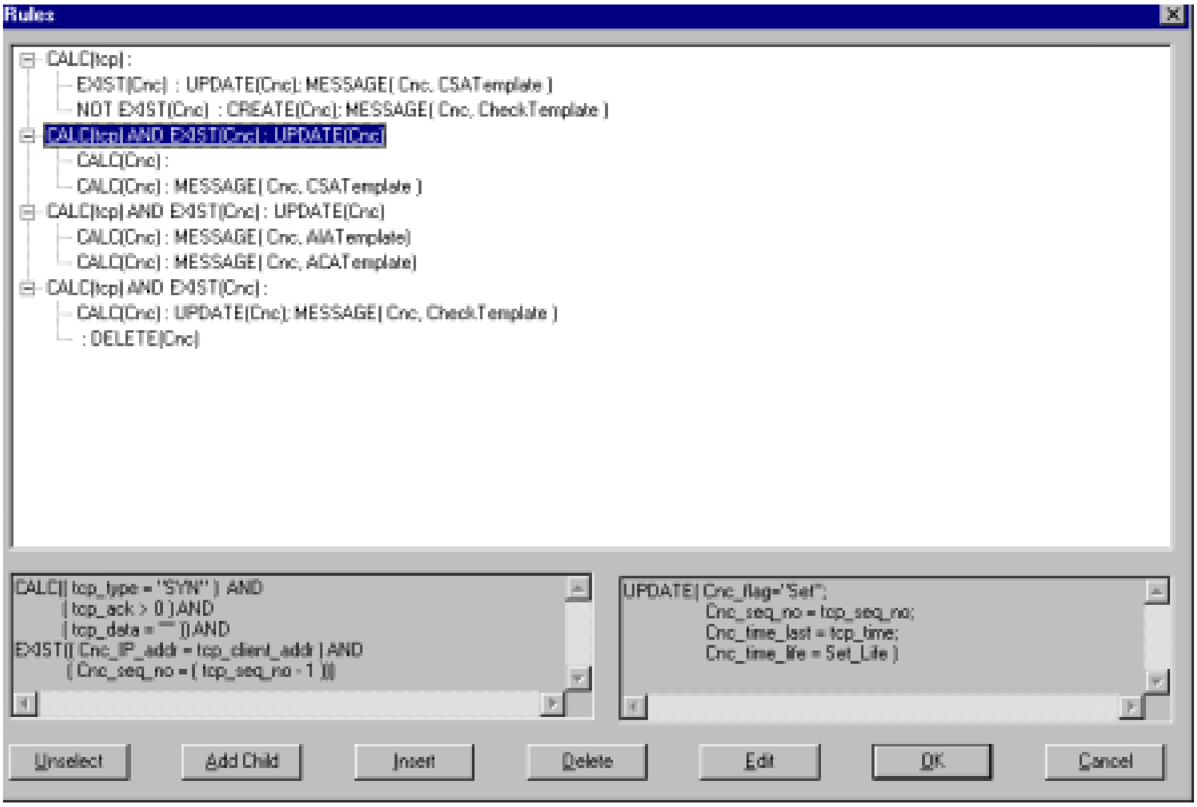


Fig.A.3. Common scheme of the agent *AD-E* operation

Script A. Common scheme of preprocessing of the obtained tcp-messages



```
CALC[tcp] :
    EXIST[Cnc]  : UPDATE[Cnc]; MESSAGE[ Cnc, CSATemplate ]
    NOT EXIST(Cnc]  : CREATE[Cnc]; MESSAGE[ Cnc, CheckTemplate ]
CALC[tcp] AND EXIST[Cnc] : UPDATE[Cnc]
    CALC[Cnc] :
    CALC[Cnc] : MESSAGE[ Cnc, CSATemplate ]
CALC[tcp] AND EXIST[Cnc] : UPDATE[Cnc]
    CALC[Cnc] : MESSAGE[ Cnc, AIATemplate]
    CALC[Cnc] : MESSAGE[ Cnc, ACATemplate]
CALC[tcp] AND EXIST[Cnc] :
    CALC[Cnc] : UPDATE[Cnc]; MESSAGE[ Cnc, CheckTemplate ]
     : DELETE[Cnc]
```

```
CALC[[ tcp_type = "SYN" ] AND
        [ tcp_ack > 0 ] AND
        [ tcp_data = "" ]] AND
EXIST[[ Cnc_IP_addr = tcp_client_addr ] AND
        [ Cnc_seq_no = [ tcp_seq_no - 1 ]]]
```

```
UPDATE[ Cnc_flag='Set';
            Cnc_seq_no = tcp_seq_no;
            Cnc_time_last = tcp_time;
            Cnc_time_life = Set_Life ]
```

Fig.A4. Rules of the input tcp-messages preprocessing

Fig.A.4 represents four generalized rules of the agents' class *AD-E* behavior (see upper window).

A.1. The rule determines that the input tcp-message with a flag Syn is obtained, this message corresponds to a new connection establishment (the generalized condition of this rule is shown in Fig.A.4, line 1 in the upper window). According to this rule two decision variants are realized depending on various conditions.

A.1.1. The input tcp-message with a flag Syn is obtained, this message corresponds to a new connection establishment from the part of some host H, concerning to a defended network (generalized condition and action of this rule are shown in Fig.A.4, line 2 in the upper window). The *agent - demon* has information that the attack "Denial of service" is accomplished on the host H. The record in the form "current connection" in this agent's database (see table A.2) testifies this fact. This record was registered in an agent's database during execution of the behaviour rule C.1 of the same agent (see below). As a result of the obtained message processing a modification of the available record about current connection is fulfilled (see table A.2), and this information is addressed to the agent *IDA1* on the same host.

Table A.2.

	Initial record	Modification of the record attributes
ID	-	Current N + 1
IP address	Tcp (Client.address)	=
Port destination	-	Tcp (Server.port)
Flag	-	HOC
Last sqn_no	-	Tcp (sqn_no)
Access	-	-
Time on	-	Tcp (time)
Time last tcp	-	Tcp (time)
Time life	-	Ack_wait_time
Fact	Denial of service	Connect imitation
Data	-	-

Designations: - - the value is not defined, = - a former value.

A.1.2. The obtained input tcp-message with a flag Syn corresponds to a new connection establishment (see Fig.A.4, line 3 in the upper window). The registration record of a new connection (table A.3) is generated in the agent's database in a format of the concept "Current connection", and this information is transferred to the agent *AD-P1*.

Table A.3.

ID	Current N + 1
IP address	Tcp (Client.address)
Port destination	Tcp (Server.port)
Flag	HOC
Last sqn_no	Tcp (sqn_no)
Access	-
Time on	Tcp (time)
Time last tcp	Tcp (time)
Time life	Ack_wait_time
Fact	-
Data	-

A.2. The rule determines, that the input tcp-message with a flag Ack is obtained, this message corresponds to the last phase of "hand shake" (see Fig.A.4, line 3 in the upper window and also contents of two windows below, this rule is marked). On the basis of a sequence number a record appropriate to this connection is found in a database, and on the basis of parameters of the obtained message a modification of this record is fulfilled (table A.4).

Table A.4.

	Modification of the record attributes
ID	=
IP address	=
Port destination	=
Flag	Set connection
Last sqn_no	sqn_no + 1
Access	-
Time on	=
Time last tcp	Tcp (time)
Time life	Connection life time
Fact	=
Data	-

A.2.1. The field *Fact* of current connection does not contain any data (Fig.A.4, line 5 in the upper window). This condition corresponds to normal connection.

A.2.2. The value of the field *Fact* of current connection is Denial of service (Fig.A.4, line 6 in the upper window). In this case the value of the field *Fact* varies on *Connect imitation*, and this information is transferred to the agent *IDA1*.

A.3. The rule determines that the tcp-message transmitting the data is obtained (see a Fig.A.4, line 7 in the upper window). On the basis of the message sequence number in a data base a record appropriate to this connection is found, and on the basis of the obtained message parameters a modification of this record attributes (table A.5) is fulfilled.

Table A.5.

	Modification of the record attributes
ID	=
IP address	=
Port destination	=
Flag	=
Last sqn_no	Tcp (sqn_no)
Access	=
Time on	=
Time last tcp	Tcp (time)
Time life	Connection life time
Fact	=
Data	Tcp (data)

A.3.1. The rule determines that the connection is in a status *Set connection*, and dispatches to agent *AIA* the message about the connection, including data from a field data of the input *tcp*-message (see Fig.A.4, line 8 in the upper window).

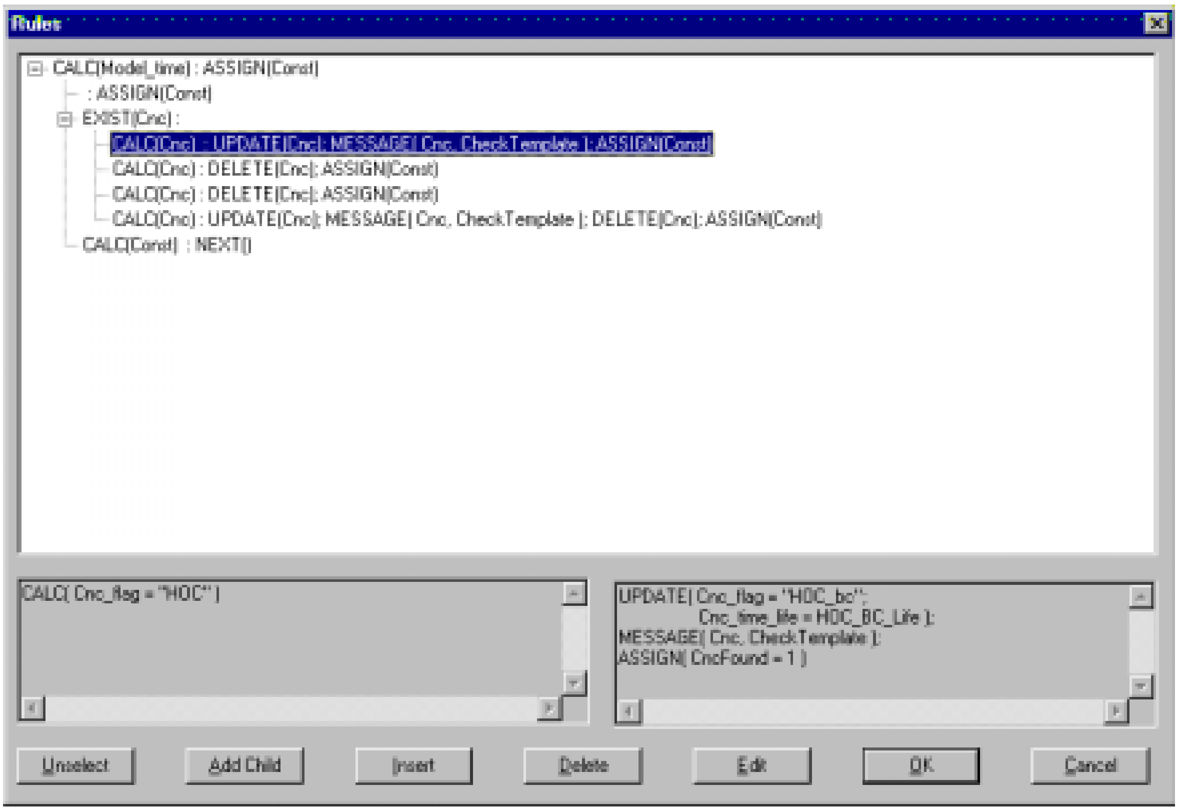
A.3.2. The rule determines that the connection is in a status *Login*. Besides the rule dispatches to agent *ACA* the message about the connection, including data from a field data of the input *tcp*-message (see Fig.A.4, line 9 in the upper window).

A.4. The rule determines that the *tcp*-message with a flag Fin is obtained, this message corresponds to the connection closing (see Fig.A.4, line 10 in the upper window). On the basis of the message sequence number a record appropriate to the connection is found in a database.

A.4.1. The rule determines that the connection is in a status *Set connection* (see Fig.A.4, line 11 in the upper window). In this case the value *Empty connection* is assigned to attribute *Fact* in a record about the connection and the information about a connection is transferred to the agent *AD-P1*.

A.4.2. The record about the connection is deleted from the agent's database (see Fig.A.4, line 12 in the upper window). If the description of the connection contains any detected fact of non-authorized actions, then the information on the completed connection is recorded in archive of the completed connections.

Script B. Supervision of a life time of the connections in current statuses



```
CALC[Model_time] : ASSIGN[Const]
    : ASSIGN[Const]
    EXIST[Cnc] :
        CALC[Cnc] : UPDATE[Cnc]; MESSAGE[ Cnc, CheckTemplate ]; ASSIGN[Const]
        CALC[Cnc] : DELETE[Cnc]; ASSIGN[Const]
        CALC[Cnc] : DELETE[Cnc]; ASSIGN[Const]
        CALC[Cnc] : UPDATE[Cnc]; MESSAGE[ Cnc, CheckTemplate ]; DELETE[Cnc]; ASSIGN[Const]
    CALC[Const] : NEXT[]
```

```
CALC[ Cnc_flag = "HOC" ]
```

```
UPDATE[ Cnc_flag = "HOC_bc";
        Cnc_time_life = HOC_BC_Life ];
MESSAGE[ Cnc, CheckTemplate ];
ASSIGN[ CncFound = 1 ]
```

Fig.A.5. Rules of the time stamps processing

B.1. The condition of the rule determines that the message on a current value of the model time is obtained (see Fig.A.5, line 1 in the upper window).

B.1.1. The rule sets the order of execution of the subsequent rules of this level in a decision tree (see Fig.A.5, line 2 in the upper window).

B.1.2. The rule discovers the first record about the connection, in which the connection life time is delayed in a current status (a selection condition is *Exist Connect*, *where time_last_tcp* + *life_time* > *current_time*) (see Fig.A.5, line 3 in the upper window).

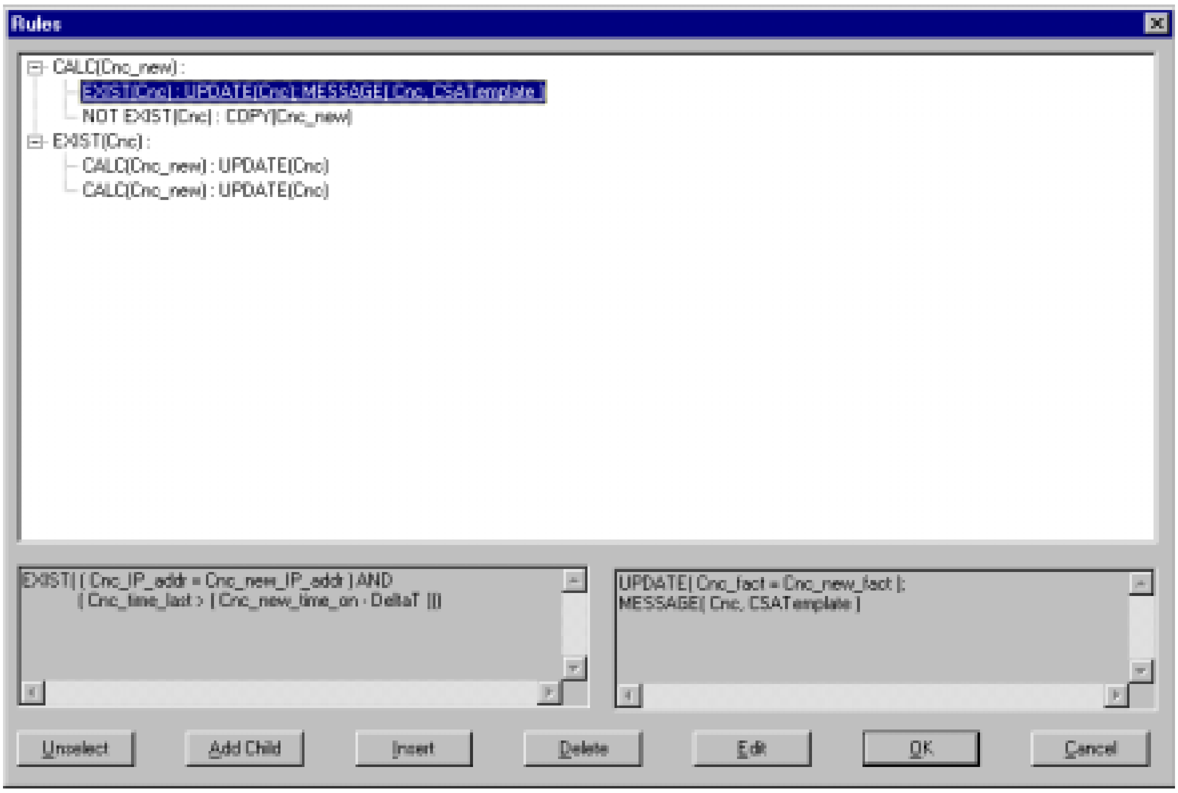
B.1.2.1. The connection from a status *HOC (Half open connection)* is transferred in a status *Bad connection*, the appropriate life time value is assigned to the attribute *Life_time*, and the message on the connection status is transferred to the agent *AD-P1* (see Fig.A.5, line 4 in the upper window and also contents of two windows bellow, this rule is marked).

B.1.2.2. The connection from a status *Set connection* is transferred to the status *Bad set connection* and this information is transmitted to the agent *AD-P1*, then the record about the connection is deleted from a database and is recorded in archive of the completed connections (see Fig.A5, line 5 in the upper window).

B.1.2.3. The connection is in a status *Log*. In this case a record is deleted from a database (see Fig.A.5, line 6 in the upper window).

B.1.2.4. The connection from a status *Set connection* is transferred to *BSC (Bad set connection)* and this information is transmitted to the agent *AD-P1*, then the record about the connection is deleted from a database and is recorded in archive of the completed connections (see Fig.A.5, line 7 in the upper window).

Script C. Responses on the facts about the connections



```
⊟ CALC[Cnc_new] :
    EXIST[Cnc] : UPDATE[Cnc]; MESSAGE[ Cnc, CSATemplate ]
    NOT EXIST[Cnc] : COPY[Cnc_new]
⊟ EXIST[Cnc] :
    CALC[Cnc_new] : UPDATE[Cnc]
    CALC[Cnc_new] : UPDATE[Cnc]
```

```
EXIST[ ( Cnc_IP_addr = Cnc_new_IP_addr ) AND
        ( Cnc_time_last > ( Cnc_new_time_on - DeltaT )) ]
```

```
UPDATE[ Cnc_fact = Cnc_new_fact ];
MESSAGE[ Cnc, CSATemplate ]
```

Fig.A.6. Rules of the registration of the detected facts in connections

C.1. The rule determines that the message (from the agent *AD-P1* of other host) about detection of attack Denial of Service has come (see Fig.A.6, line 1 in the upper window). The message arrives in the format of table A.6.

C.1.1. The rule searches a record about the connection from a host H opened in a preset time interval (see Fig.A.6, line 2 in the upper window and also contents of two windows below, this rule is marked). The search of such record is fulfilled using the address of a host H and the defined time interval. If such connection is retrieved, then in appropriate record the value *Denial of service* of attribute *Fact* varies on a value *Connect imitation*.

C.1.2. The rule checks that during a preset time interval the connection from a host H was not open (see Fig.A.6, line 3 in the upper window). In this case the obtained warning is recorded in the agent's database and is used further during the rule A.1.1 execution.

Table A.6

	Initial record
ID	-
IP address	Tcp (Client.address) *Host H*
Port destination	-
Flag	-
Last sqn_no	-
Access	-
Time on	-
Time last tcp	-
Time life	-
Fact	Denial of service
Data	-

C.2. The rule determines that the answer message from the agent *AIA* about the identification and authentication results has come (see Fig.A.6, line 4 in the upper window).

C.2.1. The value of a flag *Log* in the obtained connection testifies to a successful identification and authentication (see Fig.A.6, line 5 in the upper window). In this case in the connection record of the agent's database the status flag changes to *Log*, and the access level defined by the agent *AIA* according to access control rules is assigned to attribute *Access*.

C.2.2. This case corresponds to a negative result of the identification and authentication (see Fig.A.6, line 6 in the upper window). The connection remains in the status *Set connection*, and the value *Bad login* is assigned to the attribute *Fact*.

A1.2.2. Scripts of the agent AD-P1 operation

The main function of this class agent (see Fig.A.7) is a support of a current quantity statistics of open connections for detection of the *port scanning* and *Syn flood* attack of the class *Denial of service*. Fig.A.8 can be an informative explanation of the behaviour script, defined for this agent. Formal tag of port scanning is the quantity of the connections opened from one host. The

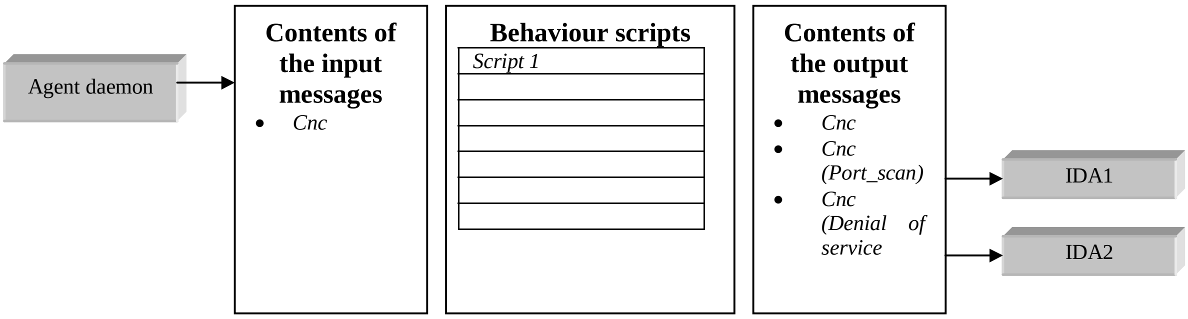


Fig.A.7. Common scheme of the agent *AD-P1* operation

conclusion about possible port scanning can be done if the connections quantity will exceed a preset threshold. This conclusion is for construction of a rule of the port scanning detection. However on this basis it is possible to generate a more exact rule taking into account variety of ports and also presence of informative actions in these connections.

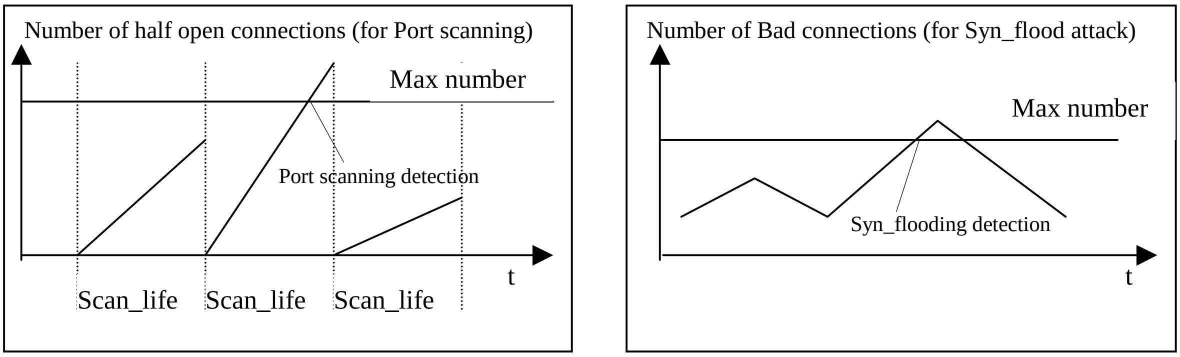

Number of half open connections (for Port scanning)
Max number
Port scanning detection
t
Scan_life
Scan_life
Scan_life
Number of Bad connections (for Syn_flood attack)
Max number
Syn_flooding detection
t

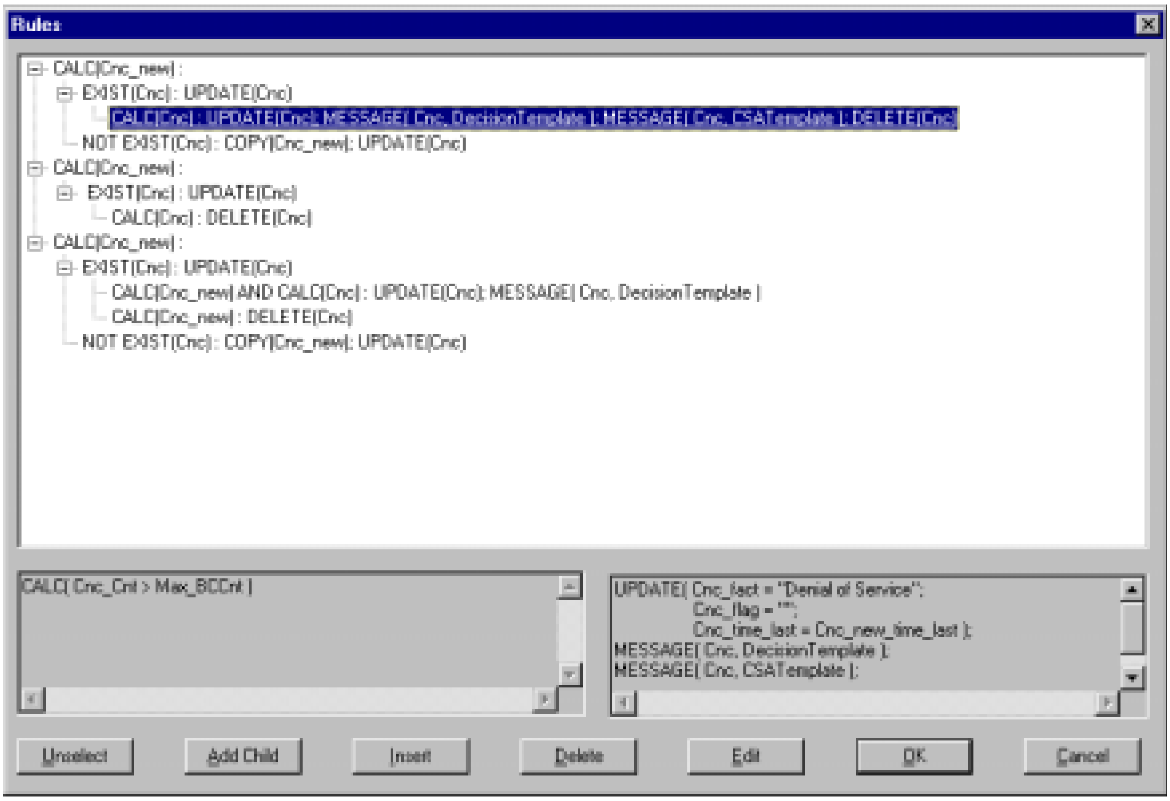
Fig.A.8. Graphical representation of rules of attack detection by the agent *AD-P1*

A formal tag of the *Syn flood* attack realization is a quantity of connections on the same port in a current instant in a status *Bad connection*. The conclusion about possible development of this attack is done if the connections quantity exceeds a preset threshold.

For construction of these detection rules an agent *AD-P1* should use the reserved attribute *N* (number of the connections possessing defined parameters) of defined concept “current connection” (see the table A.1).

Script A. The supervision of a quantity of the “bad” connections

A.1. The condition of the rule determines that the message about the connection transferred to a status *Bad connection* has come (see fig.A9, line 1 in the upper window).



```
CALC[Cnc_new] :
    EXIST[Cnc] : UPDATE[Cnc]
        CALC[Cnc] : UPDATE[Cnc]; MESSAGE[ Cnc, DecisionTemplate ]; MESSAGE[ Cnc, CSATemplate ]; DELETE[Cnc]
    NOT EXIST[Cnc] : COPY[Cnc_new]; UPDATE[Cnc]
CALC[Cnc_new] :
    EXIST[Cnc] : UPDATE[Cnc]
        CALC[Cnc] : DELETE[Cnc]
CALC[Cnc_new] :
    EXIST[Cnc] : UPDATE[Cnc]
        CALC[Cnc_new] AND CALC[Cnc] : UPDATE[Cnc]; MESSAGE[ Cnc, DecisionTemplate ]
        CALC[Cnc_new] : DELETE[Cnc]
    NOT EXIST[Cnc] : COPY[Cnc_new]; UPDATE[Cnc]
```

```
CALC[ Cnc_Cnt > Max_BCCnt ]
```

```
UPDATE[ Cnc_fact = "Denial of Service";
        Cnc_flag = "";
        Cnc_time_last = Cnc_new_time_last ];
MESSAGE[ Cnc, DecisionTemplate ];
MESSAGE[ Cnc, CSATemplate ];
```

Fig.A.9. Rules of the “bad” connections generalization

A.1.1. The rule determines that already there are connections with the same host in a status *Bad connection* and magnifies a value *N* on 1 in appropriate record of concept “current connection” (see Fig.A.9, line 2 in the upper window). For a search of the necessary record the following parameters are used: *IP address, Port destination* and a value *Bad connection* of the connection status in a field *Flag*.

A.1.1.1. If the value *N* has exceeded a preset maximum threshold, then the value *Denial of service* (*Syn Flood*) is assigned to a field *Fact*, and the instant, when the last connection has transferred to a status *Bad connection,* is recorded in a field *Time last tcp* (see Fig.A.9, line 3 in the upper window, and also contents of two windows below, this rule is marked). The message about the detected fact is transmitted to all agents *IDA1* of other hosts, and also to agent *IDA2* of the same defended host.

A.1.2. The rule determines that for the present there are no connections with the host that send message in a status *Bad connection* (see Fig.A.9, line 4 in the upper window). In this case a new record with appropriate parameters from the obtained message is registered, and the value 1 is assigned to *N*.

B.1. The rule determines that the message about the connection breaking in a status *Bad connection* on the life time has come (see Fig.A.9, line 5 in the upper window).

B.1.1. The rule discovers in the agent’s database an appropriate record and reduces the value *N* on 1 in this record (see Fig.A.9, line 6 in the upper window).

B.1.1.1. If the value N became equal 0, then the record is deleted (see Fig.A.9, line 7 in the upper window).

C.1. The rule determines that the message about the beginning of the new connection has come from some host (see Fig.A.9, line 8 in the upper window).

C.1.1. The rule discovers in the agent’s database an appropriate record and magnifies the value *N* on 1 in this record (see Fig.A.9, line 9 in the upper window). For a search of the necessary record the following parameters are used: *IP address* and the value of the connection status *Half open connection*.

C.1.1.1. The rule checks that the open connections count time has not exceeded a preset time interval, and the open connections quantity has exceeded a preset threshold (see Fig.A.9, line 10 in the upper window). If this condition appears true, then a conclusion about port scanning is generated and the message about this fact is transferred to the agent *IDA2* of the same host.

C.1.1.2. The rule checks that the open connections count time has exceeded a preset time interval (see Fig.A.9, line 11 in the upper window). In this case the relevant record is deleted.

C.1.2. This rule works if the rule C.1.1 has not found a necessary record in the agent’s database (see Fig.A.9, line 12 in the upper window). In this case a new record with parameters from the arrived message is registered, and the value 1 is assigned to *N*.

A1.2.3. Scripts of the agent *AD-P2* operation

The agent *AD-P2* is responsible for detection of attacks *Port scanning* (on an application layer), *Finger search* and *Buffer overflow* (Fig.A.10). Formal tag for these types attacks detection is a presence of a defined string in a data field of the input tcp-message addressed to the defined port. For example, under port scanning the tcp-packet field *Data* can include a substring “*expn cybercop*” at call to a port 25. The collection of examples of the similar sort possible combinations is established in the auxiliary table *PT*. One of three possible decisions is compared to each combination in this table:

- *Port scanning,*

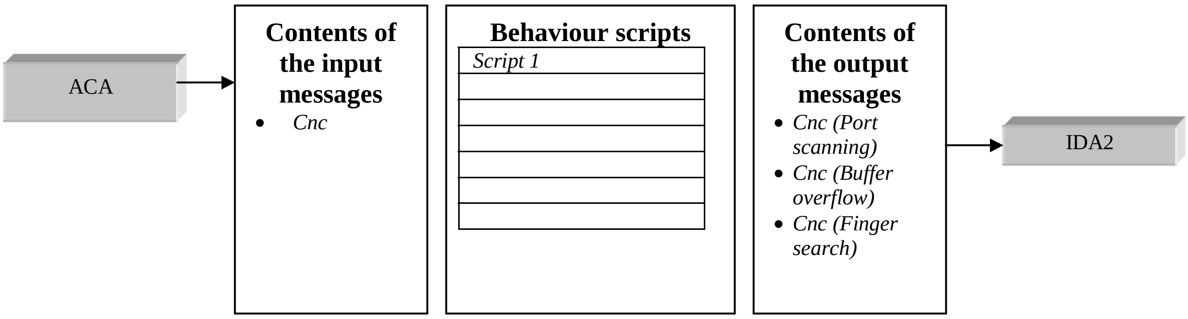
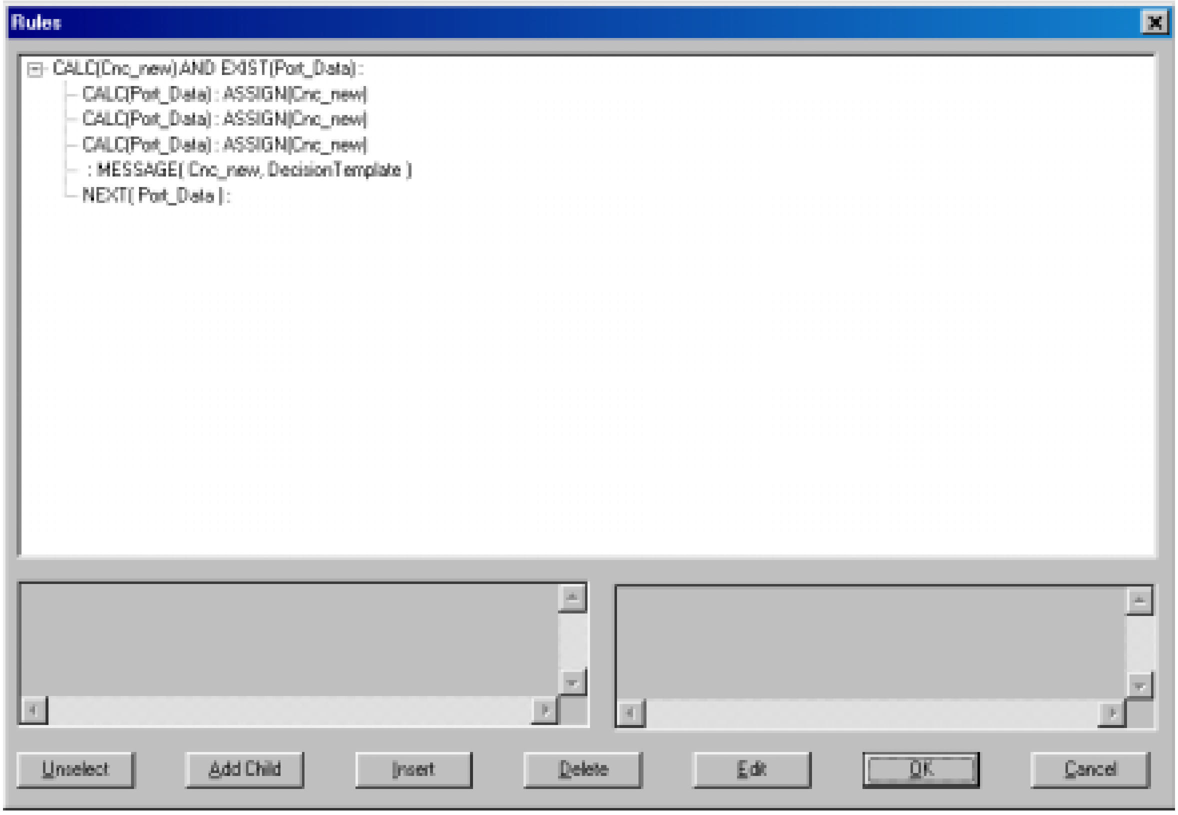


Fig.A.10. Common scheme of the agent *AD-P2* operation

- *Finger search*,
- *Buffer overflow*.



```
⊟ CALC(Cnc_new) AND EXIST(Port_Data) :
    CALC(Port_Data) : ASSIGN(Cnc_new)
    CALC(Port_Data) : ASSIGN(Cnc_new)
    CALC(Port_Data) : ASSIGN(Cnc_new)
     : MESSAGE( Cnc_new, DecisionTemplate )
    NEXT( Port_Data ) :
```

Fig.A.11. Rules of the agents *AD-P2* behaviour

A.1. The rule uses data from a description of the current connection, to which the input tcp-message concerns (see Fig.A.11, line 1 in the upper window). At this *tcp*-message preprocessing stage the actual information (in particular a port number and string from a *tcp*-packet data field) was transferred to the connection description. The rule receives these data and checks them on a presence of an identical data in the auxiliary table *PT*.

A.1.1/2/3. If the rule A1 has detected one of three enumerated attack classes, then the next three subordinate rules register this result in a field *Fact* of the current connection description (see Fig.A.11, lines 2-4 in the upper window).

A.1.4. At detection of the attack fact this rule generates the appropriate message to the agent *IDA2* (see Fig. A.11, line 5 in the upper window).

A1.2.4. Scripts of the agent *AIA* operation

The common scheme of the agent *AIA* operation is represented in Fig.A.12.

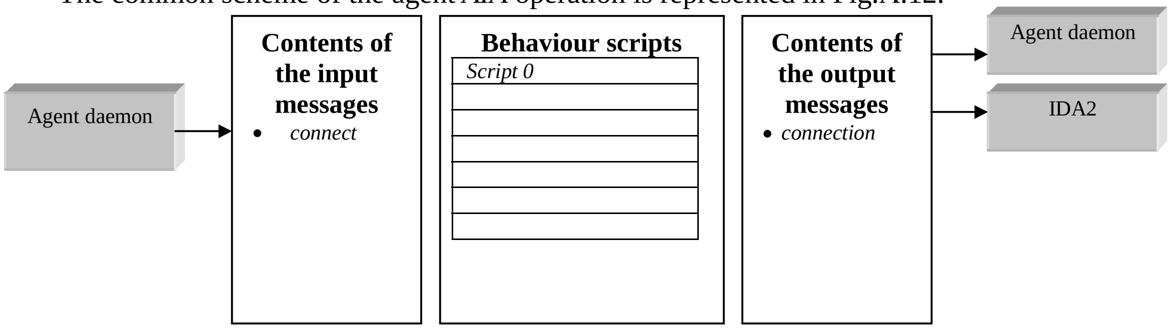
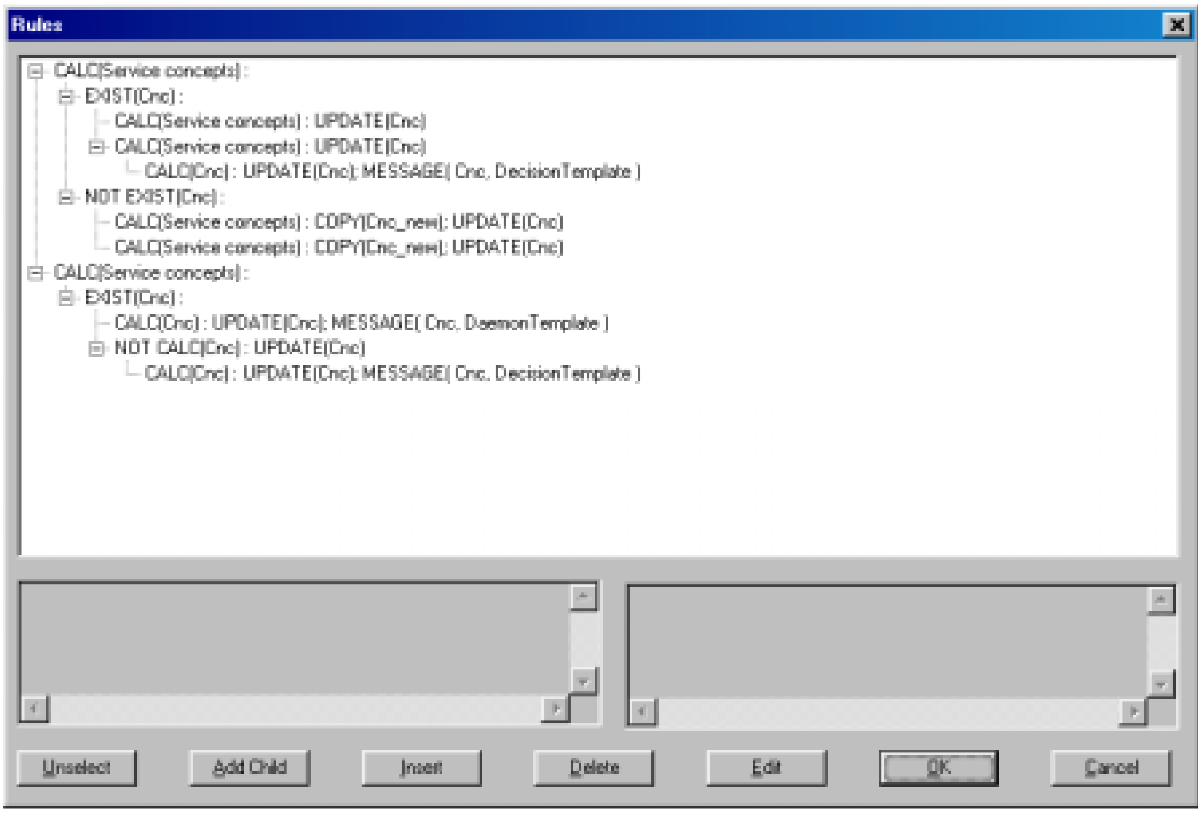


Fig.A.12. Common scheme of the agent *AIA* operation

Script A. Check of the user’s name and password



```
CALC[Service concepts] :
    EXIST(Cnc) :
        CALC[Service concepts] : UPDATE(Cnc)
        CALC[Service concepts] : UPDATE(Cnc)
            CALC[Cnc] : UPDATE(Cnc); MESSAGE( Cnc, DecisionTemplate )
    NOT EXIST(Cnc) :
        CALC[Service concepts] : COPY[Cnc_new]; UPDATE(Cnc)
        CALC[Service concepts] : COPY[Cnc_new]; UPDATE(Cnc)
CALC[Service concepts] :
    EXIST(Cnc) :
        CALC(Cnc) : UPDATE(Cnc); MESSAGE( Cnc, DaemonTemplate )
        NOT CALC[Cnc] : UPDATE(Cnc)
            CALC[Cnc] : UPDATE(Cnc); MESSAGE( Cnc, DecisionTemplate )
```

Fig.A.13. Rules of the agents *AIA* behaviour

The agents *AIA* behaviour is determined by two generalized rules A.1 and B.1. The first rule makes an identification of a login name, and the second rule checks a password.

A.1. The rule determines that an input message contains a login name (see a Fig.A.13, line 1).

A.1.1. The rule determines that an attempt of a name input for the connection establishment is not the first within the current connection (see Fig.A.13, line 2).

A.1.1.1. The rule determines that the input name is contained in the table of names of the users having the right on operation with a host (see a Fig.A.13, line 3). In this case the value *user_ok* is recorded in a field *Fact* of the current connection description.

A.1.1.2. The rule determines that the table of names of the users does not contain the input name (see Fig.A.13, line 4). In this case a value of the access attempts counter is magnified on 1.

A.1.1.2.1. If the access attempts quantity is more than a preset threshold, then a login name guessing conclusion is adduced, and a message about this fact is sent to the agent *IDA2* (see Fig.A.13, line 5).

A.1.2. The rule determines that the login name input attempt for a connection establishment is the first within the current connection (see Fig.A.13, line 6).

A.1.2.1. The rule determines that the input name is contained in the table of names of the users having the right on operation with a host (see a Fig.A.13, line 7). In this case the value *user_ok* is recorded in a field *Fact* of the current connection description. The value of the host access attempts counter remains equal 0.

A.1.2.2. The rule determines that the table of names of the users does not contain the input name (see Fig.A.13, line 8). In this case the value 1 is assigned to the access attempts counter.

B.1. The rule determines that a user’s password is in the input message data field (see a Fig.A.13, line 9).

B.1.1. The rule checks that a login name existing in the users’ names and passwords table was entered (see a Fig.A.13, line 10). This table contains the names and passwords of the users having the right on operation with a host.

B.1.1.1. The rule determines that the input password is contained in the users’ names and passwords table and corresponds to the login name input earlier (see Fig.A.13, line 11). The user’s access rights are assigned on the basis of the same table. The message about a successful access with the indication of access rights in the current connection description field *Access* is transmitted to the agent *AD-E*.

B.1.1.2. The rule determines that the input password is incorrect and magnifies the access attempts counter on 1 (see Fig.A.13, line 12).

B.1.1.2.1. If the host access attempts quantity is more than a preset threshold, then a login name and password guessing conclusion is adduced, and a message about this fact is sent to the agent *IDA2* (see Fig.A.13, line 13).

A1.2.5. Scripts of the agent *ACA* operation

The common scheme of the agent *ACA* operation is represented in Fig.A.14.

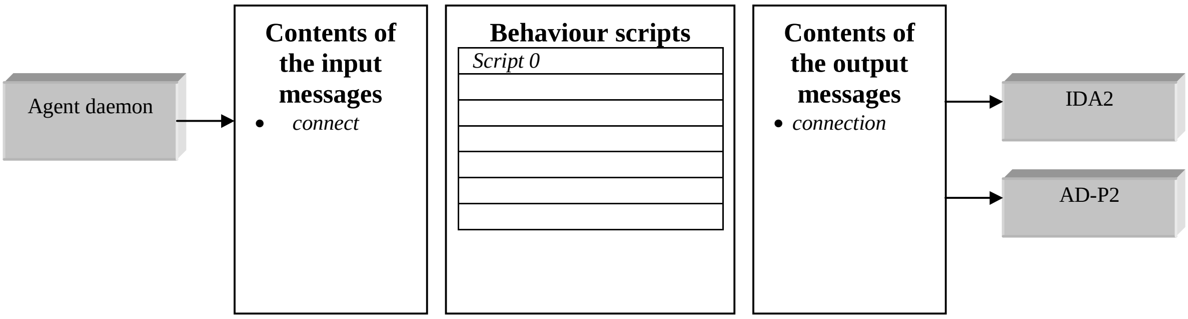
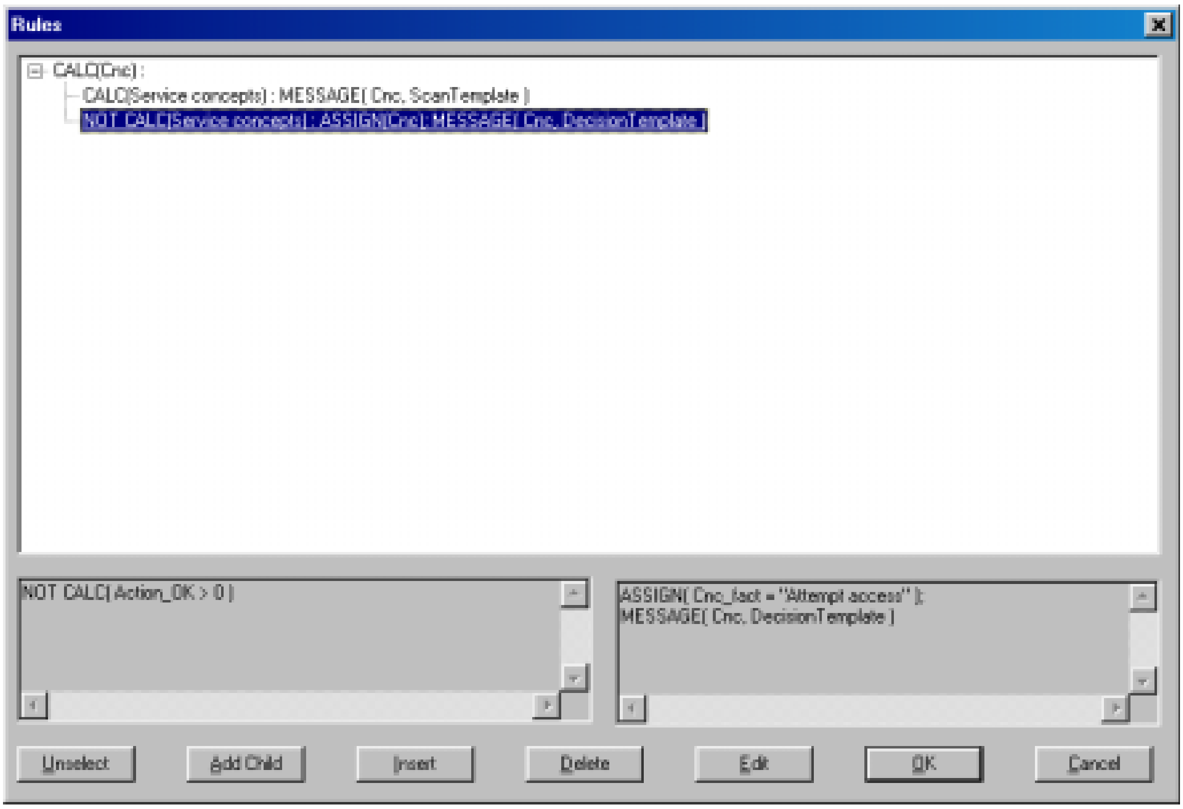


Fig.A.14 Common scheme of the agent *ACA* operation

Script A. Check of the access rights

The message including the user's access rights and the input *tcp*-message data field contents arrives to the agent *ACA* (see Fig.A.15, line 1). If the actions defined in the data field correspond to the available rights, then the first rule transmits the obtained message to the agent *AD-P2* (see Fig.A.15, line 2). If the access violation attempt is detected, then the second rule transmits this fact to the agent *IDA2* (see Fig.A.15, line 3, and also contents of two windows below, this rule is marked).



```
CALC(Cnc) :
  CALC(Service concepts) : MESSAGE( Cnc, ScanTemplate )
  NOT CALC(Service concepts) : ASSIGN(Cnc); MESSAGE( Cnc, DecisionTemplate )
```

```
NOT CALC( Action_OK > 0 )
```

```
ASSIGN( Cnc_fact = ''Attempt access'' );
MESSAGE( Cnc, DecisionTemplate )
```

Fig.A.15. Rules of the agents *ACA* behavior

A1.2.6. Scripts of the agent *IDA1* operation

The common scheme of the agent *IDA1* operation is represented in Fig.A.16.

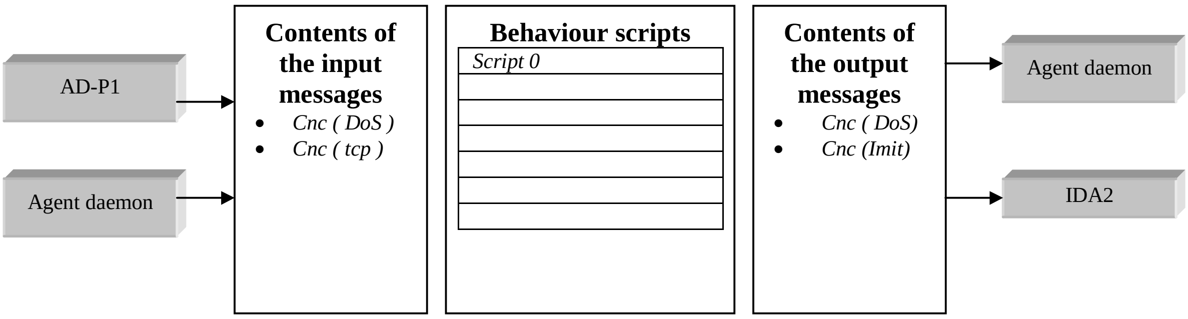
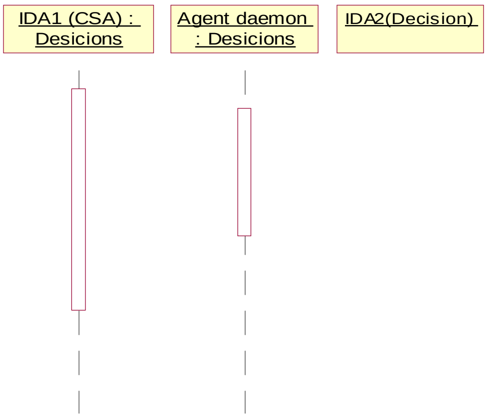


Fig.A.16. Common scheme of the agent *IDA1* operation

The agents *IDA1* fulfill the task of the *Combined spoofing attack* detection. In Case study the base mechanisms of this task decision are realized. The sequence diagram (Fig.A.17) explains an order of the agents' interaction. For implementation of a more complete task solution the following agents' dialogues is necessary to add in the scheme of the agents' interaction.



- At obtaining a message about the fact of the presumable attack *Denial of service* from a host H, the agent *IDA1* can inquire this host for a supposition confirmation.
- At obtaining the tcp-message with a flag SYN from the host undergone a *Denial of service*, the agent *IDA1* can inquire a marginal host concerning an external packet presence come simultaneously with this message.

Script A. Combined spoofing attack detection

The rules of the agent *IDA1* behaviour for the Combined spoofing attack detection are represented in Fig.A18.

A1. The rule determines that the message on the possible attack *Denial of service* is obtained (see Fig.A18, line 1). On the basis of the obtained data the rule transfers to the agent *AD-E* a message with the contents represented in the left part of the table 2 (from the description of the agents *AD-E* behaviour).

A2. This rule fixes the *tcp*-message with a flag SYN obtained from the attacked host (see Fig.A18, line 2).

A3. This rule fixes a termination of the “hand shake” on behalf of the host undergone *attack Denial of service*, and concludes a fact about an imitation of the connection on behalf of this host (see Fig.A18, line 3, and also contents of two windows below, this rule is marked). The message on the detected fact is transmitted to the agent *IDA2*.

A1.2.7. Scripts of the agent IDA2 operation

The common scheme of the agent *IDA1* operation is represented in Fig.A.19.

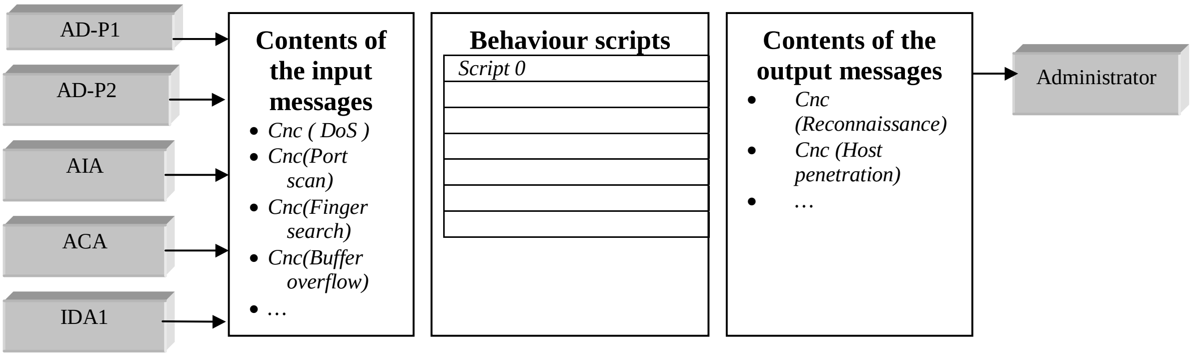
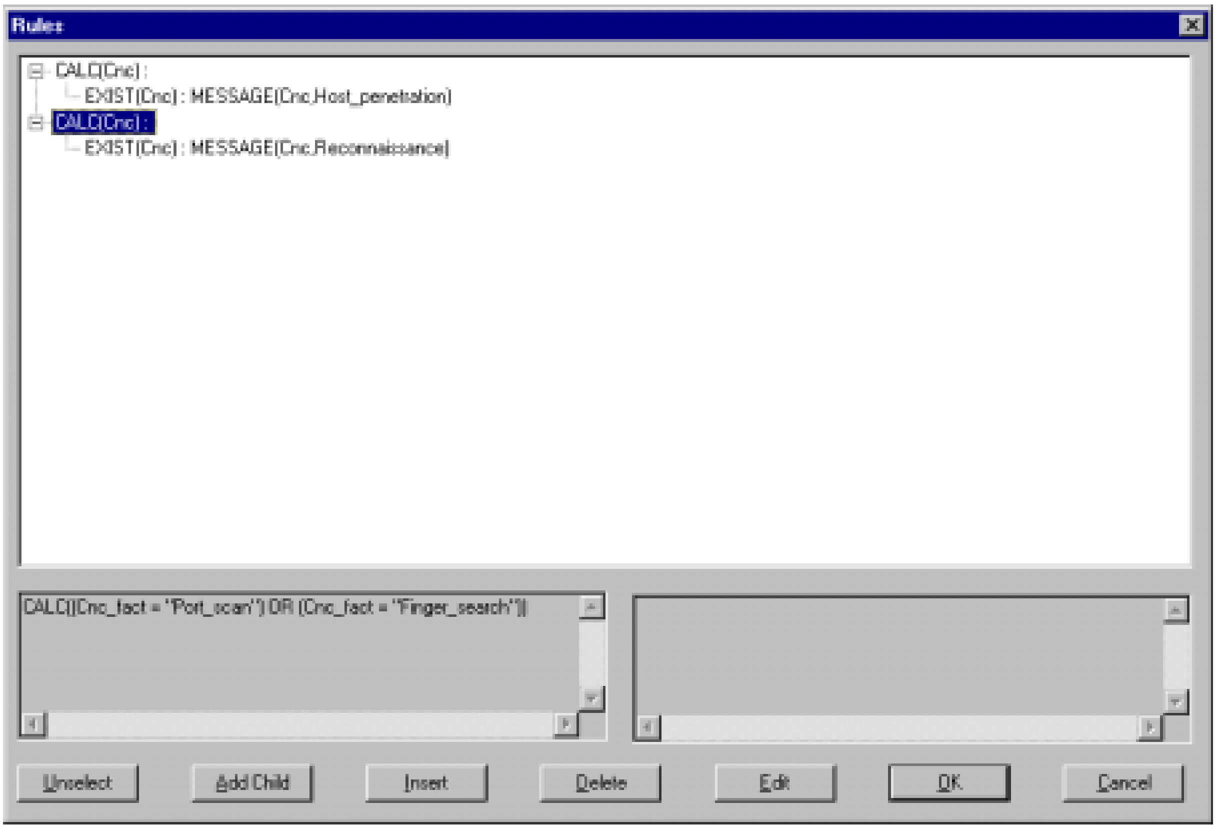


Fig.A.19. Common scheme of the agent *IDA2* operation

A.1. The rule is fulfilled, if the message about a host access attempt by a login name and password guessing or a *Combined spoofing attack* detection is arrived (see Fig.A.20, lines 1 and 2). In this case the rule parses a quantity of the similar sort facts for a preset time period. If this quantity exceeds a preset threshold, then a conclusion about a *Host penetration* is generated and the warning is dispatched to the administrator.



```
CALC[Cnc] :
   EXIST[Cnc] : MESSAGE[Cnc.Host_penetration]
CALC[Cnc] :
   EXIST[Cnc] : MESSAGE[Cnc.Reconnaissance]
```

```
CALC[[Cnc_fact = 'Port_scan'] OR [Cnc_fact = 'Finger_search']]
```

Fig.A20. Rules of the agents *IDA2* behaviour

AA.2. The rule is fulfilled, if the message about the *Port scanning* or *Finger search* facts has arrived (see Fig.A.20, lines 3 and 4, and also contents of two windows below, this rule is marked). In this case the rule parses a quantity of the similar sort facts for a preset time period. If this quantity exceeds a preset threshold, then a conclusion about a *Reconnaissance* is generated and the warning is dispatched to the administrator.